



**Internet Access for
LAN-Based Users**

Model MTPSR3-200

User Guide



User Guide

S0000004 Revision A

ProxyServer 200-Series (Model MTPSR3-200)

This publication may not be reproduced, in whole or in part, without prior expressed written permission from Multi-Tech Systems, Inc. All rights reserved.

Copyright © 1999, by Multi-Tech Systems, Inc.

Multi-Tech Systems, Inc. makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, Multi-Tech Systems, Inc. reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of Multi-Tech Systems, Inc. to notify any person or organization of such revisions or changes.

Record of Revisions

Revision	Description
A (10/22/99)	Manual released. All pages at revision A.

Patents

This Product is covered by one or more of the following U.S. Patent Numbers: **5.301.274; 5.309.562; 5.355.365; 5.355.653; 5.452.289; 5.453.986**. Other Patents Pending.

TRADEMARKS

The Multi-Tech logo and ProxyServer are registered trademarks or trademarks of Multi-Tech Systems, Inc. Adobe and Acrobat are trademarks of Adobe Systems Incorporated. Microsoft, Windows, and Windows NT are registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Multi-Tech Systems, Inc.
2205 Woodale Drive
Mounds View, Minnesota 55112
(612) 785-3500 or (800) 328-9717
Fax 612-785-9874
Tech Support (800) 972-2439
BBS (612) 785-3702 or (800) 392-2432
Internet Address: <http://www.multitech.com>

Contents

Chapter 1 - Introduction and Description

Introduction	6
Preview of this Guide	6
Front Panel	8
Back Panel	9
Link 1 (2 and 3) Connector	9
Ethernet 10Base-T Connector	9
Ethernet 10Base-2 Connector	9
Command Connector	9
Power Connector	9
Specifications	10
Ethernet Port	10
Command Port	10
WAN Links	10
Electrical/Physical	10
Requirement	10

Chapter 2 - Installation

Introduction	12
Unpacking	12
Cabling	13
Adding RAM	14

Chapter 3 - Software Loading and Configuration

Loading your Software	16
IP Wizard Setup	19
WAN Link(s) Setup	20
Setting Up Your Remote User Database	22

Chapter 4 - ProxyServer Software

Introduction	26
Before You Begin	26
Proxy Setup	27
Changing IP Parameters	28
Changing WAN Port Parameters	31
Link Usage Control Group	31
Dynamic Bandwidth Allocation	32
MLPPP	36
Port Type	38
Changing Internet Parameters	39
Enabling the DHCP Server	41
Adding ProxyServer Applications	42
Enabling the Virtual Server	44
Enabling Remote Servers	47
Telnet/TFTP	47
WEB Server	47
Running Diagnostics	49
Running Statistics	50

Chapter 5 - Client Setup

Introduction	52
Before you Begin	52
Configuring in Windows 98/95	53
Installing TCP/IP (Win98/95)	60
Configuring in Windows NT	61
Installing TCP/IP (WinNT)	67

Chapter 6 - RAS Dial-Out Redirector

Introduction	70
Installing and Configuring the WINMCSI Modem-Sharing Software	70
Running the WINMCSI Workstation Software	76

Chapter 7 - Remote Configuration

Introduction	80
Remote Configuration	80

Chapter 8 - ProxyServer Management

Introduction	84
ProxyServer Telnet Server Menu	84
Dial-Out	85
ProxyServer Management	85
ProxyServer Configuration	86
Remote User Database	86
Web Browser Management	87

Chapter 9 - Service, Warranty and Tech Support

Introduction	90
Limited Warranty	90
On-line Warranty Registration	90
Tech Support	91
Recording ProxyServer Information	91
Contacting Tech Support via E-mail	91
Service	92
The Multi-Tech BBS	93
To log on to the Multi-Tech BBS	93
To Download a file	93
About the Internet	94
Ordering Accessories	94

Appendices

Appendix A - Cabling Diagrams	96
Appendix B - Script Commands	97
Appendix C - Regulatory Information	99
Appendix D - AT Command Summary	102
Appendix E - TCP/IP	109

Glossary of Terms

Index

Proxy*Server* 200-Series

Chapter 1 - Introduction and Description

Introduction

Welcome to Multi-Tech's new ProxyServer 200-Series, model MTPSR3-200, a single, secure gateway that provides multiple LAN users with high performance Internet access. The ProxyServer functions as a TCP/IP proxy server that resides on the outer edge of your firewall and provides up to 150K of bandwidth to LAN users. The MTPSR3-200 supports dial in Remote Access Server (RAS), RAS Dial-Out Redirector, and can act as an asynchronous Gateway.

The MTPSR3-200 ProxyServer features a 10Base-T or 10Base-2 port for local LAN connection, Command Port for configuration, and three internal V.90/K56flex™ modems* with Multilink Point-to-Point Protocol (MLPPP) allowing for a bandwidth up to 150 Kbps.

The MTPSR3-200 supports client and site filtering, dial-in remote access from a PPP client, includes Network Address translation (NAT) allowing corporate web, FTP, and mail servers access from the Internet, dials on-demand for link establishment as Internet services are requested, and handles HTTP, FTP, POP3, DNS, NNTP, TFTP, IRC, SMTP, Gopher, Finger, rlogin, and Citrix requests. Optionally, your MTPSR3-200 bonds bandwidth on a single account for up to three modems using MLPPP technology.

System management is provided through the command port using bundled Windows® software which provides easy-to-use configuration menus.

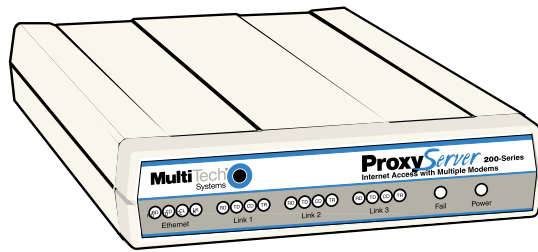


Figure 1-1. ProxyServer

Preview of this Guide

This guide describes the ProxyServer and tells you how to install and configure the unit. The information contained in each chapter is as follows:

Chapter 1 - Introduction and Description

This chapter describes the ProxyServer 200-Series. It defines the front panel indicators, back panel connections, lists technical specifications, and describes a typical Internet configuration.

Chapter 2 - Installation

This chapter provides information on unpacking and cabling your ProxyServer. The installation procedure describes each cable connection which includes connecting the power cord, Command port, LAN, and the WAN.

Chapter 3 - Software Loading and Configuration

This chapter details the software loading which configures the IP port and default WAN links. The ProxyServer software is Windows-based. Each field within a dialog box that is alterable is described.

* Though this modem is capable of 56 Kbps download performance, line impairments, public telephone infrastructure and other external technological factors currently prevent maximum 56 Kbps connections.

Chapter 4 - ProxyServer Software

This chapter describes the ProxyServer 200-Series software package designed for the Windows environment. The ProxyServer Program Group has five icons that allow for ProxyServer configuration, Download Default Setup, Download Firmware Update, Configuration Port Setup, and WAN device configuration from the program manager. Each field within a dialog box is explained in detail and when fields relate to each other, that relationship is explained.

Chapter 5 - Client Setup

This chapter provides information for enabling and configuring multiple Windows 98/95 or NT® PC users for Internet access via the ProxyServer.

Chapter 6 - RAS Dial-Out Redirector

This chapter describes how Multi-Tech's Remote Access Server for Microsoft network users enables users to dial out and fax out through the MTPSR3-200. It provides information on installing and configuring the WINMCSI modem-sharing software.

Chapter 7 - Remote Configuration

This chapter provides procedures for changing the configuration of a remote ProxyServer. Remote configuration allows you to change the configuration of a unit by simply connecting two modems between the two ProxyServers and remotely controlling the unit.

Chapter 8 - ProxyServer Management

This chapter describes typical Telnet Client applications (e.g., ProxyServer configuration and WAN device configuration).

Chapter 9 - Service, Warranty and Tech Support

This chapter provides instructions on getting service for your ProxyServer at the factory, a statement of the limited warranty, information about Multi-Tech's user bulletin board service, and space for recording information about your ProxyServer prior to calling Multi-Tech's Technical Support.

Front Panel

The front panel contains three groups of LEDs that provide the status of the Ethernet LAN connection, link activity, and general status of the ProxyServer. The Ethernet LAN LEDs display the activity of the LAN in whether the ProxyServer is connected to the LAN, transmitting or receiving packets, and if a collision is in progress. The Link LEDs display the status of the three links that can be connected to the ProxyServer, e.g., whether a link is ready to transmit or receive serial data or if an external communications device with a V.35 interface is connected to the ProxyServer. The General LEDs indicate whether the self test passed or failed (Note that the Fail LED is lit during boot-up) and if the power On/Off switch on the back of the ProxyServer is turned On.

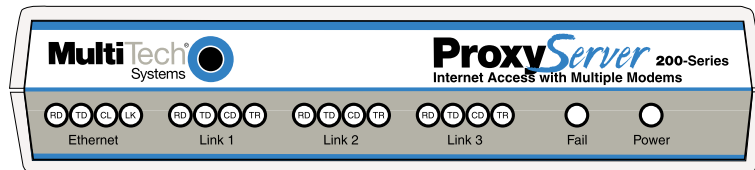


Figure 1-2. Front Panel

Ethernet

- RD** Receive Data indicator blinks when packets are being received from the local area network.
- TD** Transmit Data indicator blinks when packets are being transmitted to the local area network.
- CL** Collision indicator lights when a collision is in progress; that is, when two nodes are transmitting packets at the same time.
- LK** Link indicator lights indicating that the ProxyServer is connected to the local area network.

Links (1, 2, and 3)

- RD** Receive Data indicator blinks when the link is receiving data.
- TD** Transmit Data indicator blinks when the link is transmitting data.
- CD** Carrier Detect indicator lights when the link detects a carrier signal.
- TR** Terminal Ready indicator blinks when the link is ready to transfer data.

General

- FAIL** Fail indicator lights when a self test fails to complete as expected and during boot-up.
- POWER** The power indicator lights when the On/Off Switch is in the ON position.

Back Panel

The cable connections for the ProxyServer are made at the back panel. Three groups of cables are used on the ProxyServer, the Command Port, Link 1, 2, and 3 (RJ-11 jacks), and Ethernet. The cable connections are shown in Figure 1-2 and defined in the following groups.

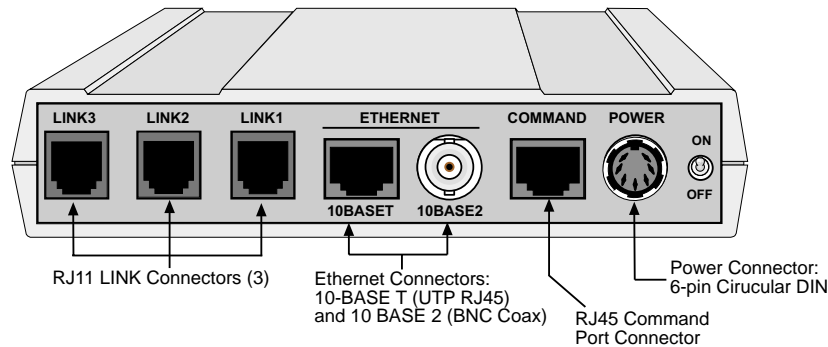


Figure 1-3. Back Panel

Link 1 (2 and 3) Connector

The Link 1, 2, and 3 connectors are used to connect the ProxyServer to a WAN. They are RJ-11 connectors.

Ethernet 10Base-T Connector

The Ethernet 10Base-T connector is used to connect the ProxyServer to a 10 MB LAN using unshielded twisted cable. This connector is an RJ-45 jack.

Ethernet 10Base-2 Connector

The Ethernet 10Base-2 connector is used to connect the ProxyServer to a LAN using thin Coax cable.

Note: The link light for Ethernet does not light when using 10Base-2.

Command Connector

The Command connector (CMD) is used to configure the ProxyServer using a PC with a serial port and running Windows software. The Command connector is an RJ-45 jack and is used with the RJ-45 to DB-9 command port cable provided with your ProxyServer. The command port is only used to connect the ProxyServer directly to the PC for local configuration and management.

Note: If your PC has a DB-25 (25-pin) serial port connector, you will need to obtain a DB-9 (9-pin, male) to DB-25 adapter. Connect the DB-25 end of this adapter to the serial port on your PC, and then connect the DB-9 (9-pin, female) end of the Command Port cable to the adapter.

Power Connector

The Power connector is used to connect the external power supply to the ProxyServer. The Power connector is a 6-pin circular DIN connector. A separate power cord is connected to the power supply and the live AC grounded outlet.

Specifications

- Protocols: Point-To-Point Protocol (PPP), MultiLink Point-To-Point Protocol (MLPPP), and Serial Line Internet Protocol (SLIP)
- Ethernet Lan Interface: 10Base-T (twisted pair) or 10Base-2 (ThinNet) BNC connector
- WAN Interface: 3 asynchronous Links (RJ-11) jacks
- Command Port: 19.2 Kbps Asynchronous
- One 1 meg by 32 bytes at 70 nanoseconds SIMM is 4 mb DRAM

Caution: SIMM speed and size cannot be mixed

Ethernet Port

- One Ethernet Interface - 10Base-T (twisted pair) RJ-45 jack or 10Base-2 ThinNet BNC connector

Command Port

- Single 19.2 Kbps asynchronous Command Port using a short RJ-45 to DB-9 cable to connect directly to PC

WAN Links

- Three internal V.90/K56flex™ modems* with MultiLink Point-To-Point Protocol for a bandwidth up to 150 Kbps

Electrical/Physical

- Voltage - 115 VAC (Standard), 240 Volts AC (Optional)
- Frequency - 47 to 63 Hz
- Power Consumption - 10 Watts
- Dimensions - 1.625" high x 6" wide x 9" deep
5.63cm high x 22.34cm wide x 33.51cm deep
- Weight - 2 pounds (.92 kg)

Requirement

- PC with Windows 3.1x or Windows 98/95 and Windows NT, and one serial COM port to connect to the Command Port of the ProxyServer

* Though this modem is capable of 56 Kbps download performance, line impairments, public telephone infrastructure and other external technological factors currently prevent maximum 56 Kbps connections.



Chapter 2 - Installation



Introduction

This chapter describes how to unpack and cable your ProxyServer. The unpacking section describes the contents of the shipping box and the installation procedure describes each cable connection and shows where that cable is connected to the ProxyServer.

Unpacking

The shipping box contains:

- ProxyServer (1)
- Quick Start Guide (1)
- ProxyServer CD with the ProxyServer Software and User Guide in Adobe Acrobat™ format (1)
- RJ-11 to phone jack cables (3)
- external power supply (1)
- RJ-45 to DB-9 Command Port cable (1)

Inspect the contents for signs of any shipping damage. If damage is observed, do not power up the unit, contact Multi-Tech's Technical Support for advice (refer to [Chapter 9](#)). If no damage is observed, place the ProxyServer in its final location and perform the cabling procedures that follow.

Save the shipping box in case reshipment is necessary.

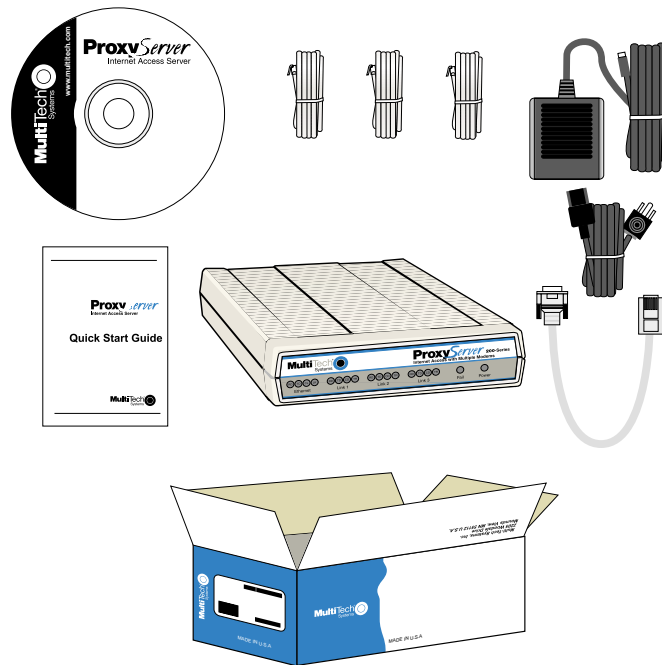


Figure 2-1. Unpacking

Cabling

The cable connections include up to three WANs, two types of connections for your Ethernet, a short adapter cable to connect to your PC for software loading, and finally your power connection. If additional RAM needs to be added, refer to the “Adding RAM” section. Figure 2-2 shows the ProxyServer’s external connections.

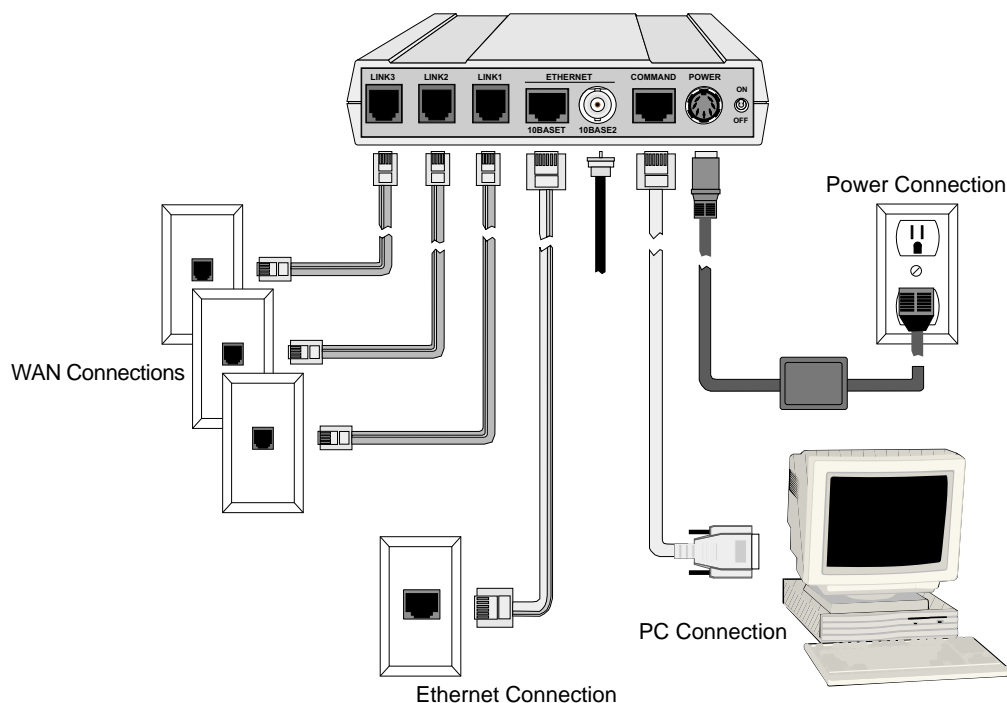


Figure 2-2. Back Panel Connections

1. Connect the external power supply to the ProxyServer and a live AC outlet. The POWER connector on the back panel of the ProxyServer is a 6-pin circular DIN connector.
2. Connect a PC running Windows® to the COMMAND port on the back panel of the ProxyServer. Use the short RJ-45 to DB-9 cable provided with your ProxyServer to connect directly to your PC, or to the serial cable from your PC.
3. Configure the ProxyServer for your application using the procedures in Chapter 3.
4. Connect a network cable to either the ETHERNET 10BASE-T (RJ-45) or a coax cable to the 10BASE-2 (BNC) port on the back panel of the ProxyServer. Connect the other end of the cable to the network.
5. Connect an RJ-11 phone cable for the first link connection to the LINK 1 port on the back panel of the ProxyServer. Connect the other end of the cable to the line jack. Connect the second RJ-11 phone cable to the LINK 2 port on the ProxyServer and the other end to the second line jack. Connect the third RJ-11 phone cable to the LINK 3 port and to the third line jack.

Adding RAM

A second SIMM connector is provided for adding RAM to the ProxyServer. Do the following.

Note: Memory should only be added when required by Multi-Tech Systems.

1. Ensure that the external power supply is disconnected from the ProxyServer.
2. Turn the ProxyServer upside down and remove the cabinet mounting screw (1) located at the center back of the cabinet (Refer to Figure 2-3).

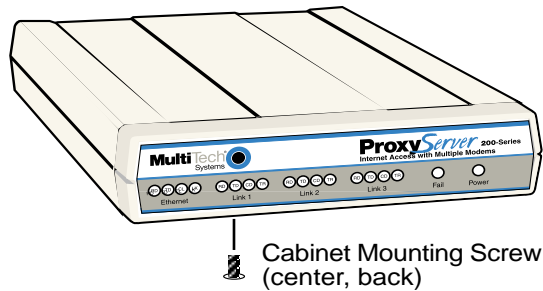


Figure 2-3. Cabinet Mounting Screws

3. Turn the ProxyServer right side up and tilt the back down slightly and the base will slide out of the cabinet.
4. Place the unit in a position where the LEDs are facing you.
5. Slant the new SIMM at a 45° angle to the back of the base and align the centering notch of the SIMM with the center tab on the SIMM connector.
6. Gently press down on the ends of the SIMM until the two latches latch over the SIMM and the two vertical pins enter the holes in the SIMM (Refer to Figure 2-4).

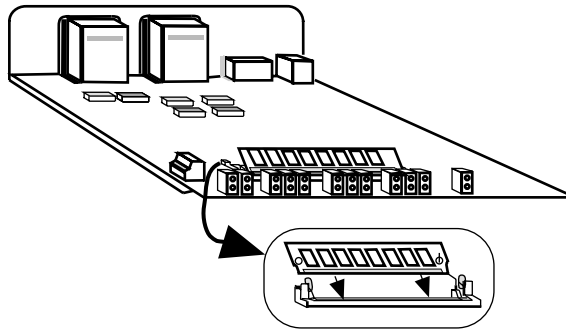


Figure 2-4. Installing a SIMM

7. Slide the base back into the cabinet with the LEDs facing toward the front and the back side grounding tabs pressing against the side of the cabinet.
8. Turn the ProxyServer upside down and replace the cabinet mounting screw (1) located toward the front of the cabinet.
9. Turn the ProxyServer right side up and connect the cables.



Chapter 3 - Software Loading and Configuration



Loading your Software

The ProxyServer Install Software and User Guide are provided on the ProxyServer CD-ROM. The CD-ROM is auto-detectable and should start automatically when inserted into your CD-ROM drive. After you have configured your ProxyServer, you can install the User Guide on your hard drive (for later viewing or printing) by clicking the Install Manuals icon on the Installation CD screen.

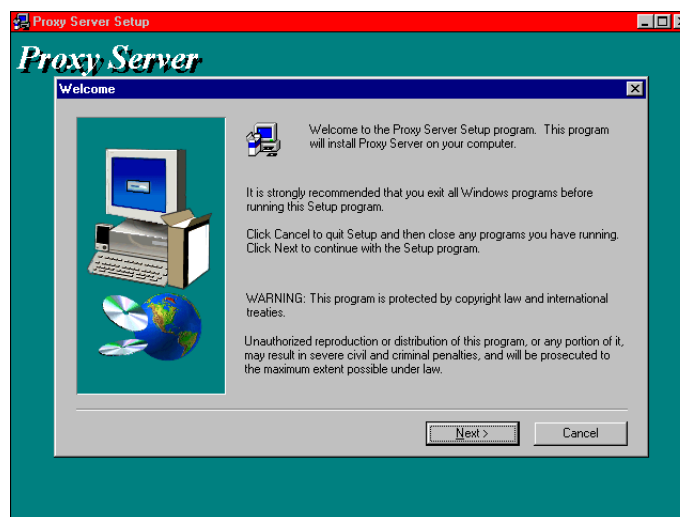
1. Before inserting the ProxyServer CD-ROM into your CD-ROM drive, determine whether you will configure your ProxyServer over the LAN or directly from a local PC. For configuring over a network, your PC must first be configured for network communications (i.e., TCP/IP stack must be installed) and both the PC and the ProxyServer must be on the same physical LAN segment. If you need to load the TCP/IP stack, refer to Chapter 5 - Windows Client Setup.
2. Insert the ProxyServer CD-ROM into a CD-ROM drive on your local PC. The CD-ROM should start automatically. However, it may take 10 to 20 seconds for the Multi-Tech Installation CD screen to appear.

The **Installation CD** screen is displayed.



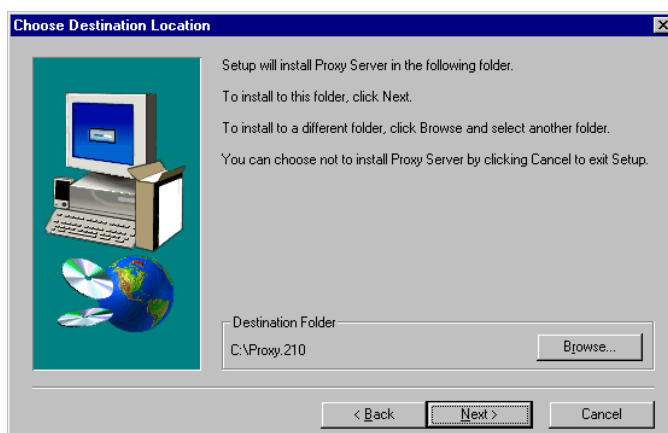
If the Multi-Tech Installation CD Screen does not appear automatically, click **My Computer**, then right-click the **CD-ROM drive icon** and click **Autorun**.

3. When the Multi-Tech Installation CD Screen appears, click the **Install Software** icon.
4. The ProxyServer Setup **Welcome** screen is displayed.



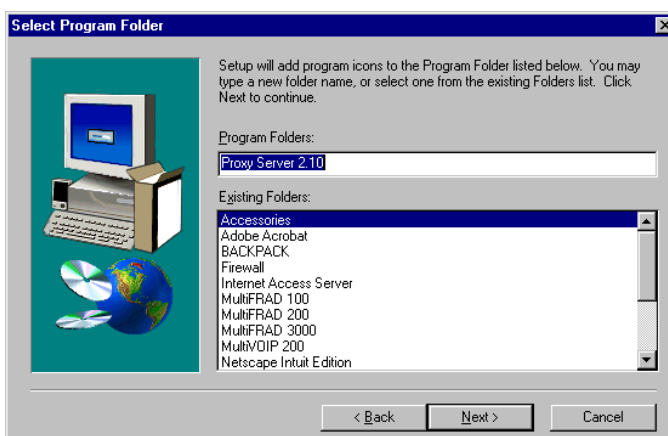
Press **Enter** or click **Next>** to continue.

- The **Choose Destination Location** dialog box is displayed. Follow the on-screen instructions to install your ProxyServer software.



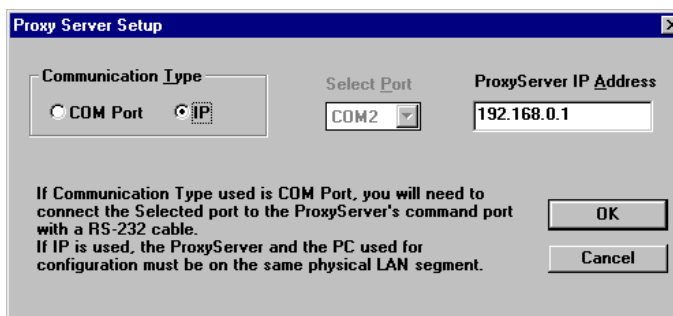
You can either choose the Destination Location of your ProxyServer software or select the default destination by clicking **Next>**. If you click **Browse**, you can select a different destination folder for your ProxyServer software; however, it is recommended that you accept the default folder, **C:\Proxy.210**.

- The **Select Program Folder** dialog box enables you to name the Program Folder for the ProxyServer files. You can select the default name, **ProxyServer 2.10**, or name it anything you like.



When finished, click **Next>** to continue.

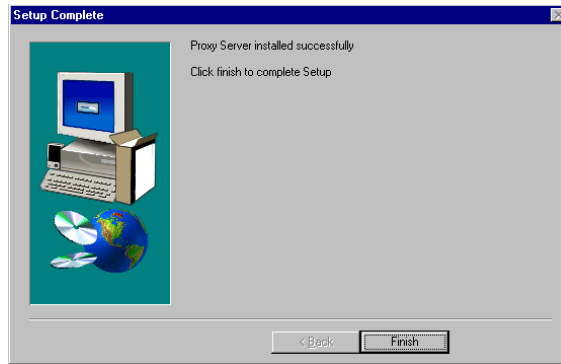
- The **ProxyServer Setup** dialog box asks if you are configuring your ProxyServer through the COM port of your PC or over the LAN (IP).



If you are configuring the ProxyServer over your network, click **OK** to continue.

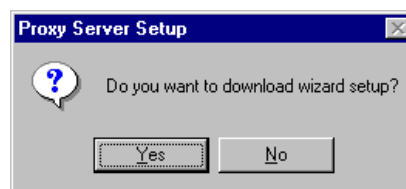
If you need to configure your ProxyServer through the Command port, follow the instructions in the dialog box for selecting the **COM Port**, then click **OK** to continue.

8. The **Setup Complete** dialog box is displayed.



Click **Finish** to continue.

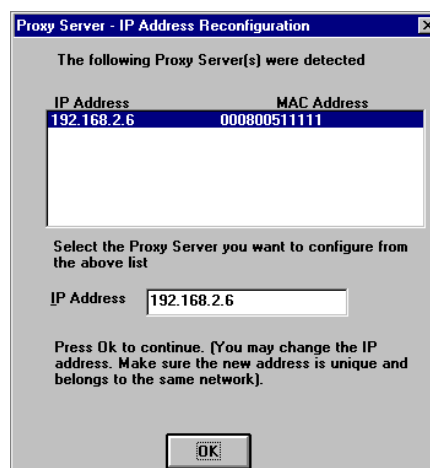
9. The “Do you want to download wizard setup?” screen is displayed.



The Wizard Setup screens enable you to input basic configuration information needed to configure your ProxyServer. These screens guide you through the process of entering your LAN address, net mask information and your WAN, DHCP Server, and Domain Name Server entries. All entries display in their respective dialog boxes when accessed from the Main menu.

Click **Yes** to download the wizard setup; clicking **No** takes you to the program group (icons) where you can choose any of eight ProxyServer utility programs.

10. If you are configuring your ProxyServer over the network, the **IP Address Reconfiguration** dialog box is displayed showing the default **IP** and **MAC addresses** of all detected ProxyServers in the top window and a suggested **IP Address** in the lower window.



From the top window, select the ProxyServer you want to configure, then verify the Suggested IP Address in the lower window.

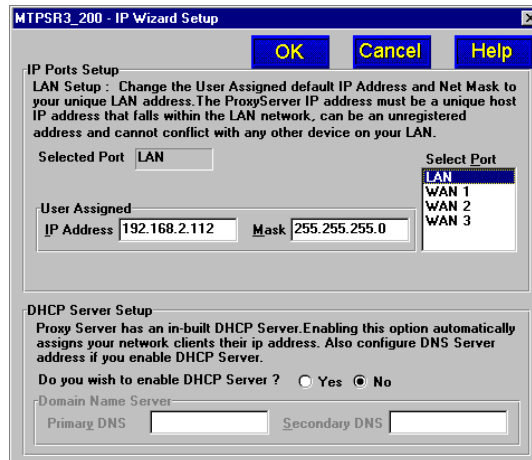
The **IP Address** is only a proposed address. You must verify that this suggested address does not conflict with the IP address of any other device currently on your network. If an address conflict exists, change the contents of this field to assign a unique address to your ProxyServer. Click **OK** when you are ready to continue.

IP Wizard Setup

The **IP Wizard Setup** dialog box guides you through the process of assigning LAN and WAN IP ports address information, and provides an option to use the ProxyServer's built-in DHCP Server if your LAN is not already running a DHCP Server which assigns (automatically) client IP addresses. If you choose to enable the built-in DHCP server, you are given the option of also enabling the Domain Name Server.

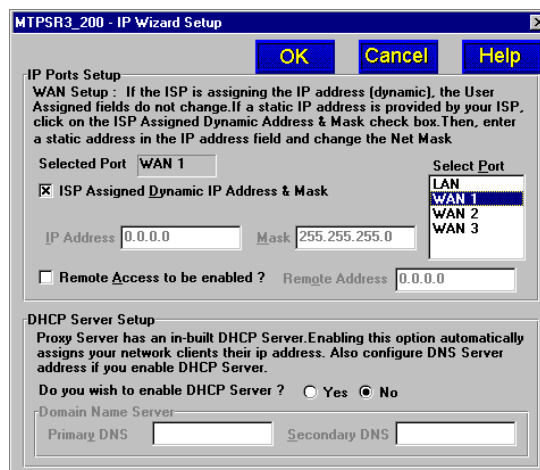
- Follow on-screen instructions to configure the IP Ports, DHCP Server, and Domain Name Server.

Note: If you plan to use the ProxyServer's DHCP server, disable any other DHCP server operating on the local/private LAN to prevent clients from receiving IP addresses from two independent sources.



If necessary, obtain Primary and Secondary DNS IP addresses from the DNS tab under Network/Protocol (or TCP/IP)/Properties or from your ISP.

- Click the **WAN 1** option in the **Select Port** window and the dialog box changes to provide WAN Setup information.



Follow the on-screen instructions to configure WAN 1. If you choose to have one or all three WAN ports configured for Remote Access, click the Remote Access to be enabled? check box, then enter the remote workstation's IP address in the Remote Address field. This is the IP address that will be handed to remote clients.

Highlight **WAN 2** and then **WAN 3**, in turn, to configure the other WAN ports.

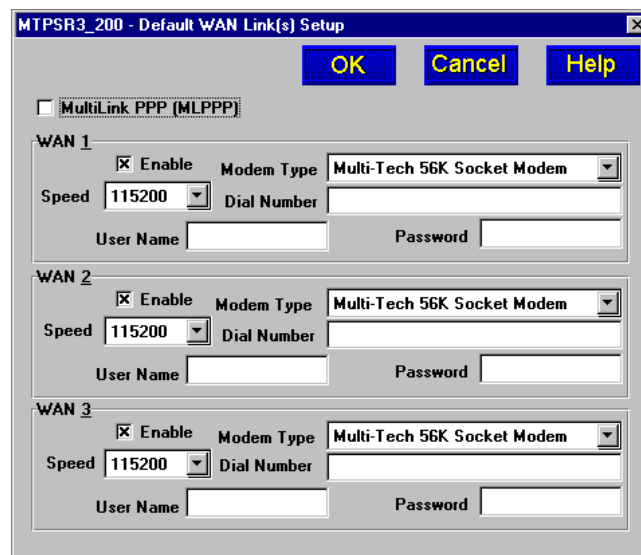
Click **OK** when you are satisfied with the IP Wizard Setup and proceed to the Default WAN Link(s) Setup screen.

WAN Link(s) Setup

The **Default WAN Link(s) Setup** dialog box guides you through bonding the WAN ports together (MLPPP), entering the phone number of the ISP, and entering your user name and password negotiated with ISP for Internet access.

13. Determine if **MultiLink PPP (MLPPP)** is going to be enabled; i.e., all three WAN links bonded together.

Note: When MLPPP is used, the Dial Number, User Name, and Password have to be the same for all three WAN ports.

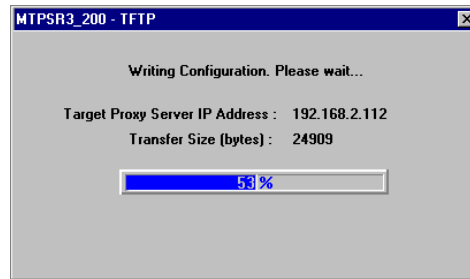


14. Click **Dial Number** for **WAN 1** and enter the phone number supplied by your ISP for WAN 1. The phone number can be a standard local number or it can include a long distance prefix.
15. Click the **User Name** for **WAN 1** and enter your user name that you negotiated with your ISP for WAN 1. The User Name can be up to 40 alphanumeric characters. The User Name is not case sensitive.
16. Click the **Password** for **WAN 1** and enter your password that you negotiated with your ISP for WAN 1. The password can be up to 15 alphanumeric characters and may or may not be case sensitive depending on your ISP.
17. Repeat the above three steps for **WAN 2**.
18. Repeat the above three steps for **WAN 3**.
19. Click the **OK** button to continue installing the software.
20. The **Checking ProxyServer** dialog box is displayed.

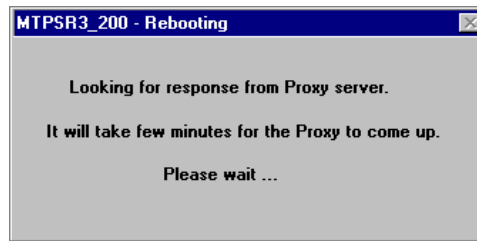


Click **OK** to proceed.

21. The **TFTP** dialog box is displayed as the configuration information is written (downloaded) to the ProxyServer.



22. During the reboot, the **Fail** LED will be on. Wait for the **Fail** LED to go off.



23. You are returned to the Multi-Tech **Installation CD** screen where you can now install (on your PC's hard drive) either Acrobat Reader (by clicking the Acrobat Reader icon) or the User Guide (by clicking the Install Manuals icon).

To install the User Guide, click the **Install Manuals** icon, select **MTPSR3-200**, and click **OK** - the files will install at **C:\Program Files\Multi-Tech Systems, Inc.\PSR3-200\Documentation**; or, you may click the **Browse** button and select an alternate directory.



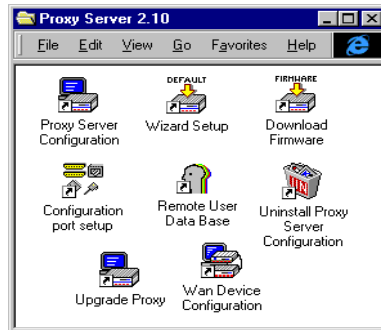
24. At this time your ProxyServer is operational; however, if DHCP is NOT being used, verify that each client PC has an IP stack loaded, workstation IP address assigned, gateway pointed to the ProxyServer, and the DNS name(s) supplied by ISP are entered. Refer to the Windows Client Setup information in Chapter 5.

Your clients are ready to access the Internet.

Setting Up Your Remote User Database

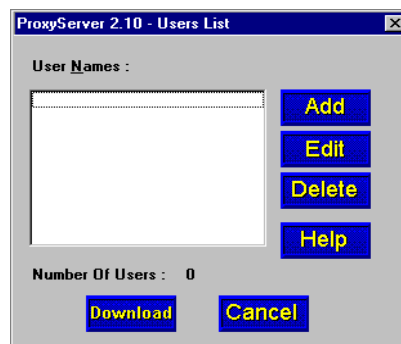
The remote user database lets you enter information about your remote users. Each WAN port can be configured as either a dial-out Proxy or a dial-in RAS. If you support remote dial-in, then the remote user database needs to be created.

1. **Win3.1 users** - From the Program Manager, click the **Remote User Data Base** icon.



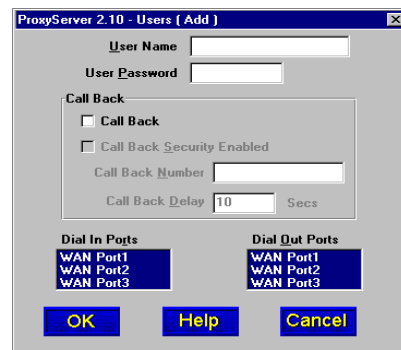
Win98/95 and WinNT users - From your desktop, click the **Start** button, point to **Programs**, then **ProxyServer 2.10**, and then click **Remote User Data Base**.

2. The **Users List** dialog box is displayed.



Click the **Add** button

3. The **Users (Add)** dialog box is displayed.



4. Build your user database by filling in the following fields for each user.

User Name.

The User Name can have as many as 39 characters. All printable characters are permitted with the restriction that a blank cannot appear in the user name. The user name is treated as a case insensitive string in dial-in and dial-out applications.

User Password.

The User Password can have as many as 7 characters. In places where the password is used as a character string, it is treated as a case insensitive string. Elsewhere (PPPs CHAP), it is treated as a case sensitive pattern.

Call Back Security Enabled

This parameter is of use in dial-in applications where the user is required to be called back at a specific location. Enabling this parameter results in having the administrator assigning the callback parameters. Disable this if the user is to be permitted to *choose* the callback number and callback delay.

Call Back Number

The callback number is editable only if callback security is enabled. This is the number where the user will be called back. The user **cannot** choose the location where he wants to be called back.

Call Back Delay

Call back delay is editable only if callback security is enabled. This specifies the duration after which the user will be called back at the administrator-assigned number.

Protocols

This lets you select the protocol(s) in which the user is allowed to dial into the ProxyServer.

Dial In Ports

This allows you to select the port over which the user is permitted to dial into the ProxyServer.

Dial Out Ports

This allows you to select the port over which the user is permitted to dial out from the ProxyServer.

5. As each user is defined in your database, click the **OK** button and the **Users List** dialog box is displayed. Click the **Add** button to continue adding users to your database.
6. When you have added all your users to the data base, from the **Users List** dialog box, click the **Download** button to load the database into the ProxyServer.



Chapter 4 - ProxyServer Software



Introduction

This chapter describes the ProxyServer software and explains how to make changes to the configuration of your ProxyServer. The major configuration parameters were established during the loading of the software (Chapter 3). The ProxyServer software and configuration utilities allow you to make changes to that initial configuration.

The ProxyServer software allows you to refine your configuration based on your network connections. The software is based on a main menu (Proxy Setup) that allows you to consider all the parameters for a particular feature (e.g., Internet access, DHCP Server addressing, and Virtual Server mappings). These features, along with others are discussed in detail in the ProxyServer Configuration section later in this chapter.

The other five configuration utilities offer additional functionality. **Wizard Setup** guides you through the initial configuration and software downloading, as described in Chapter 3. **Download Firmware** allows you to download new versions of firmware when enhancements become available. The **Configuration Port Setup** utility allows you to change the method by which you access the ProxyServer (i.e., direct connection of a PC to the Command Port on the ProxyServer, or via your Internet connection to the LAN port on the ProxyServer). The **Uninstall ProxyServer Configuration** utility is designed to remove the software from your PC. The **WAN Device Configuration** utility allows you to configure the three WAN ports. The **Remote User Data Base** option allows you to enter information regarding your remote users; and, the **Upgrade Proxy** feature allows you to download software updates from Multi-Tech System's FTP site.

Note: The **WAN Device Configuration** utility is supported only if you are directly connected to the ProxyServer. This Utility is not supported when accessing the ProxyServer via the network.

Your ProxyServer software includes the ProxyServer on-line Help system. The Help is designed to be context sensitive. Clicking the Help button within a given dialog will provide definitions and recommended values for each button, option, and field for that dialog. In some instances, you will also be presented with a list of related topics that can be displayed by clicking the green, underlined text. In addition, you can search the entire Help system (via the Index tab) for definitions and references to specific terms, fields, and recommended values where applicable.

Before You Begin

The ProxyServer software operates in a Microsoft Windows environment. Your ProxyServer program group contains all of the utilities described above, and is accessible in Windows by clicking **Start | Programs | ProxyServer 2.10 | (utility)**, or by double-clicking the utility icon in the program group in My Computer. The program group is shown here:



Proxy Setup

All changes to your ProxyServer configuration are initiated through the **Proxy Setup** dialog box or Main menu. To view or change your ProxyServer configuration in Windows 98/95 and Windows NT, click **Start | Programs | ProxyServer 2.10 | ProxyServer Configuration**. You can also start the ProxyServer Configuration from **My Computer** by double-clicking the **Proxy.210** folder on your local drive, then double-clicking on the **Roucon.exe** file. After loading, the **Proxy Setup** menu will appear.



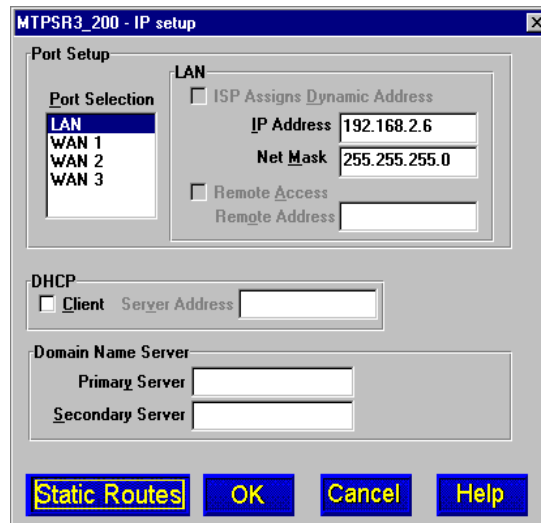
The **Proxy Setup** menu consists of 13 buttons, eleven of which allow you to display and change the IP settings, define the WAN ports, change features such as the Internet, DHCP Server, ProxyServer, and Virtual Servers, display Statistics on the WAN ports, control activation of Telnet, TFTP, and WEB servers and dumb terminal management, test the communications link, print messages received from the target ProxyServer, and download setup information to the ProxyServer.

In addition to the Statistics button, the two other buttons on the bottom row allow you to open the on-line Help system and end (Exit) a Proxy configuration session.

Note: Pressing the **Built-In Test** button displays the **Diagnostics** dialog box which allows you to perform certain hardware tests on the LAN and WAN links. The **Print Console** option brings up the console terminal that displays any print message received from the ProxyServer.

Changing IP Parameters

The **IP Setup** dialog box displays the IP addressing for your LAN and WAN ports that were established during your initial configuration. The IP Setup dialog box allows you to change any of the original parameters.



The IP Setup dialog box displays the unique LAN address and net mask you established during your initial configuration. If you are using your ProxyServer in an Internet application with one or more of the WAN ports connected to the Internet and your ISP is dynamically assigning addresses to those WAN ports, then you will want to leave the **ISP Assigns Dynamic Address** option active.

If you wanted to change a WAN port to support a static IP address, you would select the WAN port and disable the **ISP Assigns Dynamic Address** option. This activates the IP Address and Net Mask fields for that WAN port. You then need to enter a static IP address in the **IP Address** field and assign an appropriate net mask in the **Net Mask** field. Then you would want to check the WAN Setup dialog box and establish the Port Type for the selected WAN port, e.g., if the WAN port is being used for remote access you would want to enable the **RAS Enable** option and if the port is being used as a dial in feature, you would want to enable the **Dial in Only** option in the Port Type group.

If you wanted to change a WAN port to dial out to a telephone number other than the Internet, you would select the WAN port and disable the **ISP Assigns Dynamic Address** option. This activates the IP Address and Net Mask fields for that WAN port. You then need to enter a WAN port IP address in the **IP Address** field and assign an appropriate net mask in the **Net Mask** field. You would then need to check the WAN Setup dialog box and change the Port Type for the selected WAN port to enable the **Dial Out** option and enable the Asynchronous Gateway (**AG Enable**) option.

If you wanted to change a WAN port to be available for remote access, you would select the WAN port and disable the **ISP Assigns Dynamic Address** option. This activates the IP Address and Net Mask fields for that WAN port. You then need to enter a WAN port IP address in the **IP Address** field and assign an appropriate net mask in the **Net Mask** field. You would then need to check the WAN Setup dialog box and change the Port Type for the selected WAN port to enable the **Dial In** option and enable the Remote Access Server (**RAS Enable**) option.

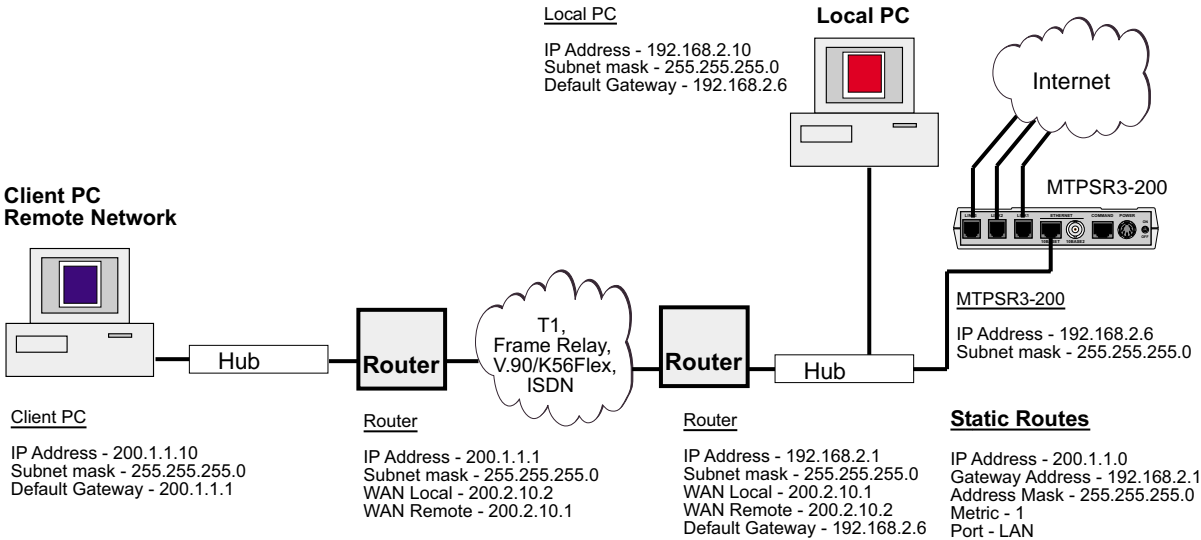
The **DHCP** (Dynamic Host Configuration Protocol) group allows IP addresses to be assigned by a DHCP Server. In such cases, a PPP client connected to the WAN port will be on the same IP network as the LAN port. Because the DHCP Server automatically assigns an IP Address for a PPP client coming up on a "Client Only" WAN port, this feature can save IP addresses that otherwise would have been taken up by the WAN port.

To enable DHCP, you must check the **Client** box and enter the IP address of the external DHCP Server (e.g., Microsoft's DHCP feature) in the **Server Address** field. The Server Address is assigned by your systems administrator.

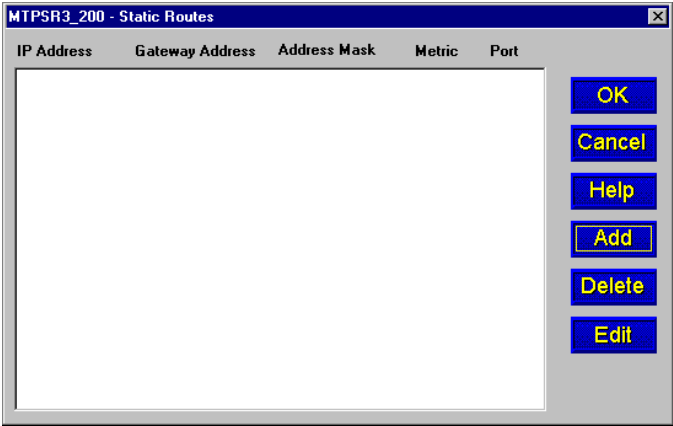
The **Domain Name Server** (DNS) group is used to resolve Fully Qualified Domain Names (FQDN) to an IP address. This field can either be filled in or left blank. If it is left blank, your ISP will assign a DNS address. This DNS address will also be handed off to any client obtaining an IP address from the ProxyServer's DHCP Server.

The **Primary Server** field defines the IP address of the first host that the ProxyServer will attempt to connect to upon a user request. If this server is unavailable, the ProxyServer will attempt a connection with the Secondary Server (if defined). The **Secondary Server** field defines the IP address of the DNS server for cases where the primary server is unavailable.

The **Static Routes** feature allows a remote client PC access to the Internet through a pre-defined route (static route). Static routing is normally used when a part of an internetwork can only be reached by one particular path. Static routes are manually configured routes that specify the transmission path a data packet must follow based on the data packet's destination address. In the example below, a data packet sent from the remote client PC to access the remote Internet through the MTPSR3-200 must have IP Address 200.1.1.0 and Gateway Address 192.168.2.1 (entered as the Static Route configuration). This determines the return path the data packet will take back to the client PC.



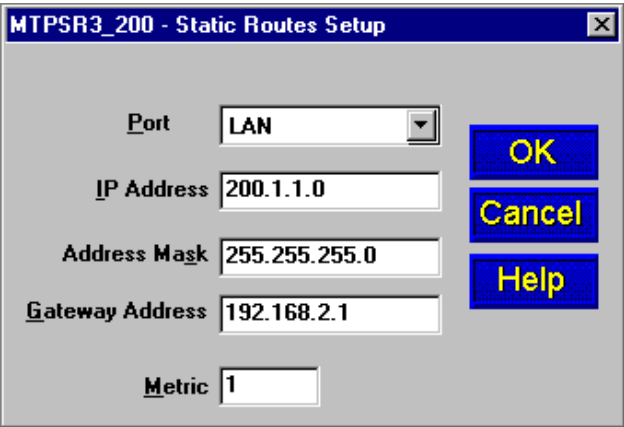
From the **IP Setup** dialog box, click the **Static Routes** button to display the **Static Routes** dialog box.



Click **Add** to display the **Static Routes Setup** dialog box where you can configure a new static route.

Note: You can also edit or delete static routes by clicking the **Edit** or **Delete** buttons.

The **Static Routes Setup** dialog box is displayed. Select and key in the appropriate information for setting up the static route.

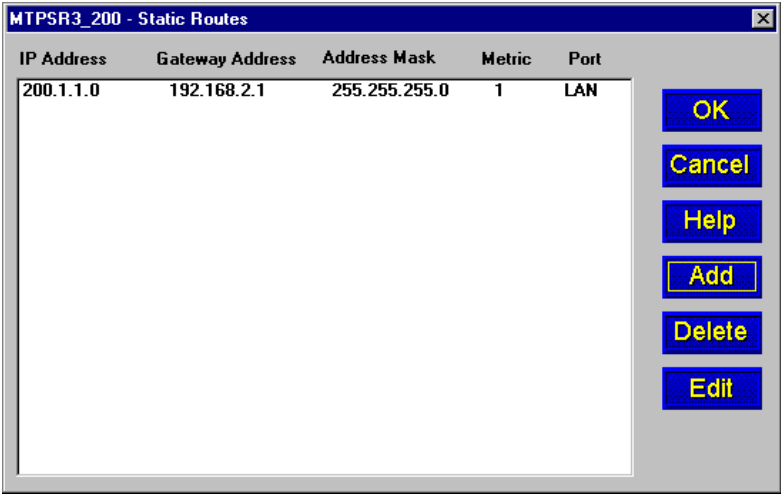


The dialog box titled "MTPSR3_200 - Static Routes Setup" contains the following fields and buttons:

- Port:** A dropdown menu with "LAN" selected.
- IP Address:** A text box containing "200.1.1.0".
- Address Mask:** A text box containing "255.255.255.0".
- Gateway Address:** A text box containing "192.168.2.1".
- Metric:** A text box containing "1".
- Buttons:** "OK", "Cancel", and "Help" are located on the right side.

Port is the type of port, usually LAN (If you have a modem connected to one of the WAN ports and are using it for RAS, you could set up a static route to route incoming traffic to a different network) . The **IP Address** must be the address of the target host or network in the static route (In our example, Static Route IP Address 200.1.1.0 indicates that PC clients on Routers with IP addresses beginning with 200.1.1 will be included on the static route). The **Address Mask** is the IP subnetwork mask (255.255.255.0) of the target host. The **Gateway Address** must be the IP address of the local router (Gateway Address 192.168.2.1) on the next hop toward the target host and the port (i.e., LAN) with which it is associated. **Metric** is the hop count (1) to the target host.

Once you have completed entering all the appropriate information, click **OK**. The static route is entered in the Static Routes table.



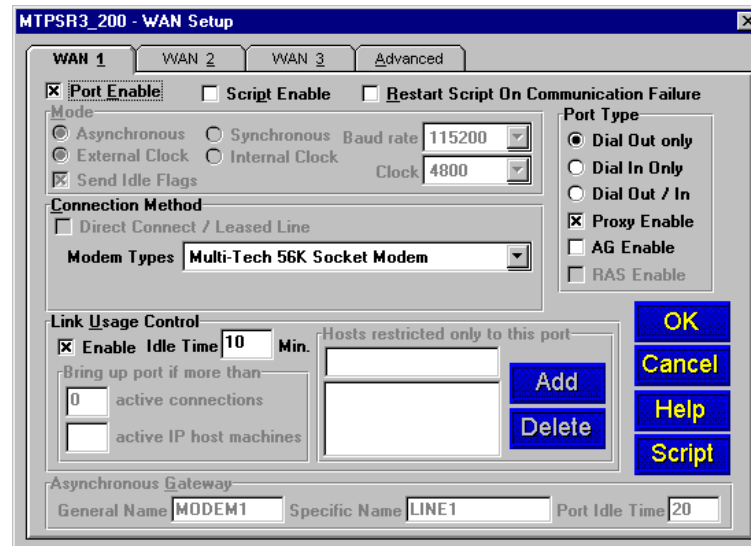
The dialog box titled "MTPSR3_200 - Static Routes" displays a table with the following data:

IP Address	Gateway Address	Address Mask	Metric	Port
200.1.1.0	192.168.2.1	255.255.255.0	1	LAN

Buttons on the right side include "OK", "Cancel", "Help", "Add", "Delete", and "Edit".

Changing WAN Port Parameters

The ProxyServer is designed to provide the flexibility needed to meet today's application needs. The **WAN Setup** dialog provides the controls for WAN configuration. Each WAN port can be configured independently of the others, or they can be combined depending on your application needs. Beyond the basic controls offered in the **Mode** and **Connection Method** groups (described in detail in your on-line Help system) the WAN Setup menu includes many advanced features.



The sections that follow detail the function of those features and provide examples of how they can be put to use. In addition, where relevant, they detail how certain features affect other dialogs in the Proxy software.

Link Usage Control Group

Note: The Link Usage Control Group is not supported when using MLPPP.

The **Link Usage Control** group allows you to control the conditions and parameters of the traffic on the three WAN ports. Using the **Enable** and **Idle Time** features, you can cause the ProxyServer to drop the connection on the selected WAN port after a specified duration without activity (as defined in the Idle Time field). The default setting is enabled (checked) with an idle time of 10 minutes. If you do not wish to use this option, click to disable (uncheck) it.

The **Bring up port if more than** group allows you to configure WAN ports 2 and 3 to become active based on the level of traffic detected on the WAN links. You can configure the Proxy to bring up an additional WAN port(s) based on the number of **active connections** or on the number of **active IP host machines**. This group does not apply to WAN 1 and is therefore inactive (grayed out) when the WAN tab selected.

The ProxyServer can be configured to limit certain workstations, based on IP addresses, to a selected port using the **Hosts restricted only to this port** group. The first of the two fields in this group defines the IP address of the workstation to be restricted. To add a new restriction, enter a valid IP address of a workstation in this field and click **Add**. The new entry will appear in the list of restrictions below. This group is not applicable to WAN 1 and is therefore inactive (grayed out) when the WAN 1 tab is selected.

Beyond the actual WAN port controls, the ProxyServer includes features that enhance WAN communications and maximize bandwidth and efficiency. The next three sections, *Dynamic Bandwidth Allocation*, *MLPPP*, and *Port Type* discuss a variety of configuration options that make use of these features.

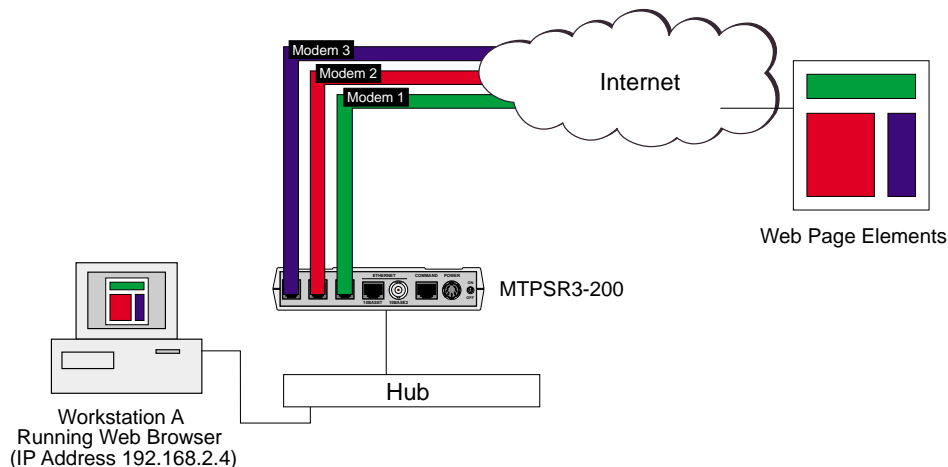
Dynamic Bandwidth Allocation

The ProxyServer uses a technology called *Dynamic Bandwidth Allocation* on its WAN ports which allows users to make use of the maximum bandwidth available during application use. In essence, this feature allows a single user to access all three WAN ports simultaneously, allowing maximized bandwidth when using a multiple stream application such as a Web browser. If a single user is utilizing all three ports, and a second user starts an application, the bandwidth is automatically re-allocated to share the WAN port resources between the users. For example, if User 1 is running a Web browser and User 2 starts a Telnet session, one of the WAN ports being used to download Web content is allocated for the Telnet session. When that session ends, the WAN port is made available to the Web browser again. All this takes place dynamically, or 'automatically' on the ProxyServer.

The examples that follow detail three different application environments that make use of dynamic bandwidth allocation. The first shows a single user downloading content from the Web. The second shows three users running various applications. The final example describes a configuration where a single WAN port is dedicated to a manager and the other two are configured for other users.

Example 1 - Single Workstation Running Web Browser

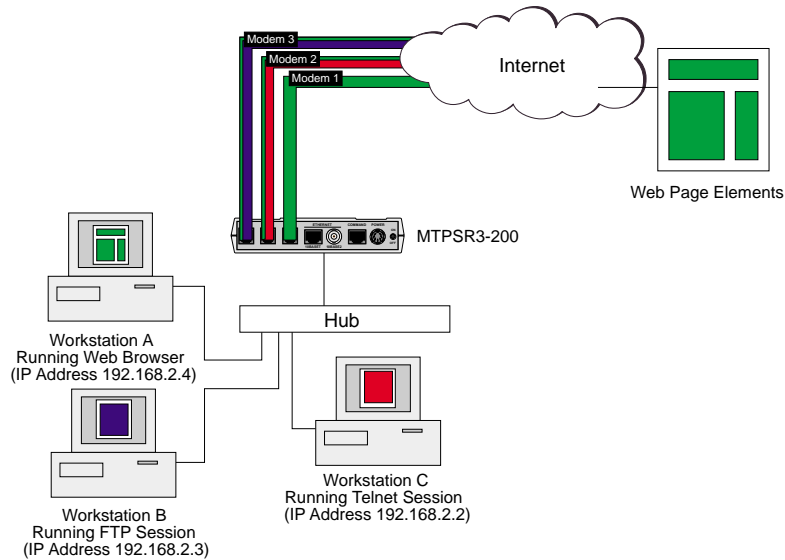
In this example, a single workstation (IP address 192.168.2.4) is using the ProxyServer with a Web browser. All three ports are available and each port can download a separate frame, therefore maximizing efficiency. Since workstation 192.168.2.4 is the only workstation actively using the Proxy, and is loading a Web page, each WAN port will download a separate frame, simulating a download of up to 150 Kps, depending on the line conditions.



If at any time another workstation requests bandwidth from the ProxyServer, the ProxyServer will shift some of the bandwidth to accommodate the requesting application. Once that application is finished, all bandwidth is re-allocated to the first workstation. For a more detailed description of this process, refer to Example 2.

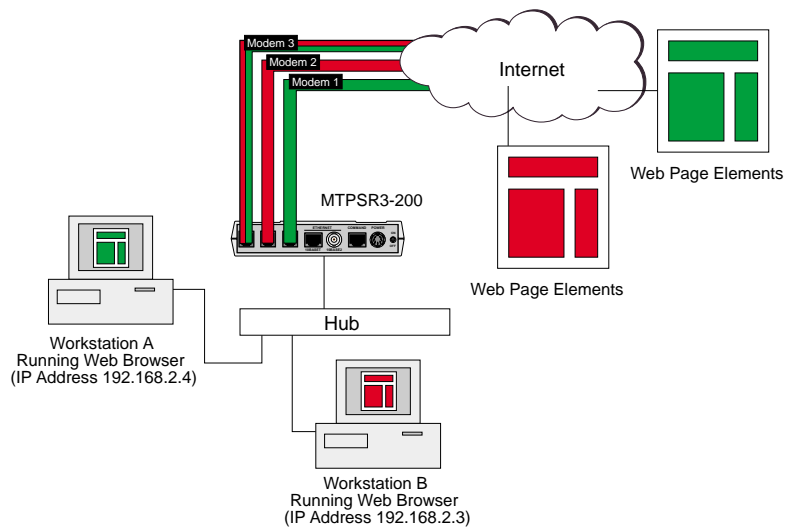
Example 2 - Multiple Workstations Running Various Applications

In Example 1 Workstation A (IP address 192.168.2.4) is loading a Web page. Example 2 shows the bandwidth allocation when two additional workstations request bandwidth from the ProxyServer. Workstation B (IP address 192.168.2.3) engages an FTP session on WAN 2, and Workstation C (IP address 192.168.2.2) engages in a Telnet session on WAN 3. Because both the Telnet and FTP sessions are single-stream applications (unlike the framed, or multiple-stream content of a Web page) they can only use one WAN port. The amount of bandwidth allocated will depend on the application and the link. If WAN 2 is connected to an FTP server providing download speeds of 19.2 Kbps, then the Web browser will load its page using WAN 1 (@ 50 Kbps) plus any "leftover" bandwidth available from WAN 2. The same applies for the Telnet session on WAN 3 - any additional bandwidth will be allocated for the Web connection.



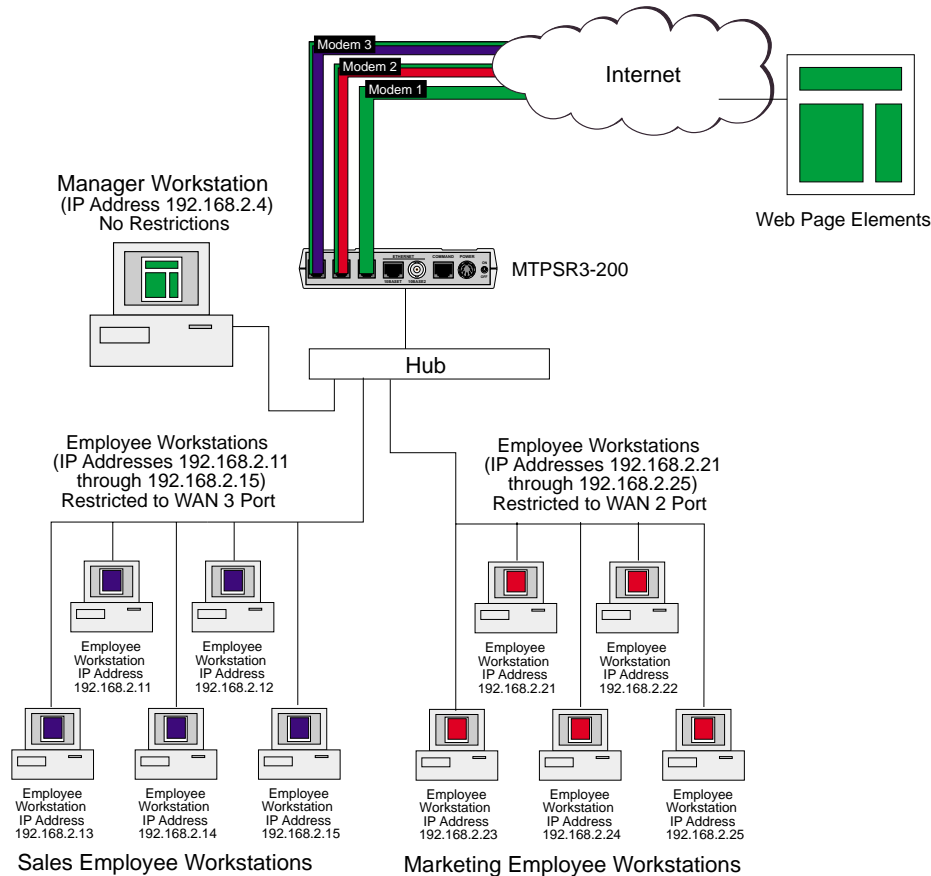
If one or both of the sessions on WAN 2 and 3 end, the ProxyServer reallocates the newly available bandwidth to the Web browser.

Another way to look at this example would be to have both Workstations A and B running Web browsers. Each workstation is downloading a separate page, but each can make use of the extra WAN port available on the Proxy. While Workstation A uses WAN 1 and Workstation B uses WAN 2, they share the extra resource available on WAN 3.



Example 3 - Single WAN Port Dedicated to Manager

In this example, a single WAN port (WAN 1) has been dedicated for exclusive use by a manager workstation (IP address 192.168.2.4). This is done by restricting all other employee workstations to either WAN 2 or WAN 3. The end result is that the manager workstation has exclusive access to WAN 1 (meaning @ 50 Kbps bandwidth automatically), plus the benefit of added bandwidth if WANs 2 and 3 are available or have “spare” bandwidth.



The configuration above shows two groups of workstations, each restricted to a specific WAN port. The Marketing Employee Workstations are restricted to WAN 2, and the Sales Employee Workstations are restricted to WAN 3. In order to do this, you need to set up the WAN ports such that each user is restricted to either WAN 2 or WAN 3. This is done through the WAN Setup dialog box.

The dialog box below shows the WAN 2 tab. In this dialog, the IP addresses for the Marketing workstations have been added to the **Hosts restricted only to this port** list. When any of these workstations launch an application, the ProxyServer will restrict its use to the WAN 2 port.

The screenshot shows the 'MTPSR3_200 - WAN Setup' dialog box with the 'WAN 2' tab selected. The 'Port Enable' checkbox is checked. Under 'Mode', 'Asynchronous' is selected with a baud rate of 115200 and a clock of 4800. 'Send Idle Flags' is checked. Under 'Connection Method', 'Direct Connect / Leased Line' is selected, and the 'Modem Types' dropdown shows 'Multi-Tech 56K Lucent Socket Modem'. On the right, 'Port Type' has 'Dial Out / In' selected, and 'Proxy Enable' is checked. The 'Link Usage Control' section has 'Enable Idle Time' checked and set to 10 minutes. The 'Bring up port if more than' section has '0 active connections' and 'active IP host machines' checked. The 'Hosts restricted only to this port' list contains the IP addresses 192.168.2.11, 192.168.2.12, 192.168.2.13, and 192.168.2.14. The 'Asynchronous Gateway' section has 'General Name' set to 'MODEM2', 'Specific Name' set to 'LINE2', and 'Port Idle Time' set to 20. Buttons for 'OK', 'Cancel', 'Help', and 'Script' are on the right.

Similarly, the dialog box below shows the WAN 3 tab with the IP addresses of the Sales workstations restricted to the WAN 3 port.

The screenshot shows the 'MTPSR3_200 - WAN Setup' dialog box with the 'WAN 3' tab selected. The settings are similar to the WAN 2 tab, but the 'Hosts restricted only to this port' list contains the IP addresses 192.168.2.21, 192.168.2.22, 192.168.2.23, and 192.168.2.24. The 'General Name' in the 'Asynchronous Gateway' section is 'MODEM3' and the 'Specific Name' is 'LINE3'. The 'Port Idle Time' remains at 20. Buttons for 'OK', 'Cancel', 'Help', and 'Script' are on the right.

MLPPP

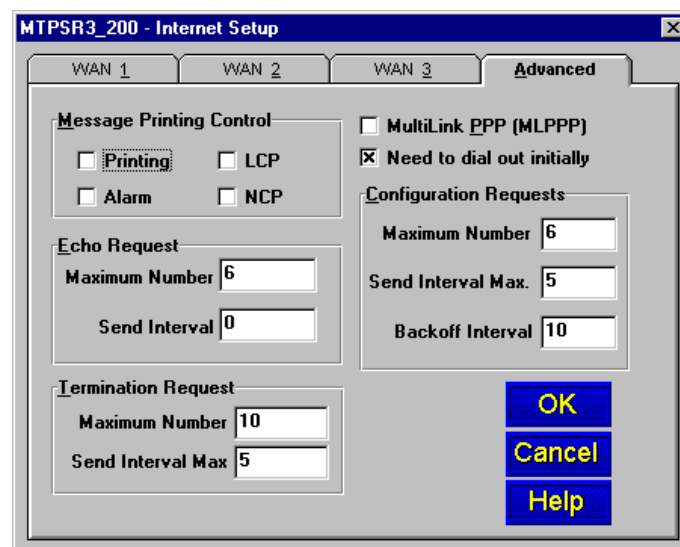
The ProxyServer supports Multi-Link Point-to-Point Protocol (MLPPP) on its WAN ports. This protocol allows the three WAN ports to act as a single pipeline using only one IP address to provide maximum bandwidth. Applications such as Telnet, FTP, and Web browsers can run a single session out of the ProxyServer and achieve up to 150K of bandwidth depending on line conditions.

In order to use MLPPP you have to enable it on the ProxyServer and have a network connection that supports it. The two primary uses would be with an Internet Service Provider (ISP) account or with a corporate site. In each case, MLPPP must be supported. Currently, not all ISPs offer MLPPP support. This is mainly because, while at the Proxy end only one IP address is required, the ISPs must provide three lines for the MLPPP connection. Most ISPs aren't willing to offer the additional lines without charging for them; however, some do support it as a "value-added" service. The more common use for MLPPP is on a corporate site running on server platforms such as Windows NT Server 4.0™ or Multi-Tech's RASExpress™, both of which have built-in MLPPP support.

In that case, the three ports are bonded together to form a 150 Kbps connection with a single IP address on the Proxy end of the link. The result is that if a workstation is engaged in an FTP session (and no other workstations are utilizing the Proxy) then that session can use the full 150K of bandwidth, far more than can be achieved on a single dedicated WAN port.

In order to use MLPPP, you must first enable it and configure the WAN ports for MLPPP. This is done using the Internet Setup dialog box and the WAN Setup dialog box.

The Internet Setup dialog box allows you to configure various parameters for the WAN ports, including protocol, and data compression. To enable MLPPP, select the **Advanced Tab**.



The master control for MLPPP is on the right-hand side of the dialog and the default setting is disabled (unchecked). To implement MLPPP, first enable (check) the **MultiLink PPP (MLPPP)** option and then determine the desired setting for the feature below it, **Need to dial out initially**. If you want the ProxyServer to dial out when you power on your Proxy, leave the default setting enabled. If you want the ProxyServer to wait to dial until it receives a dial request (i.e., from an application such as a Web browser or Telnet client) then disable (uncheck) this option.

Once MLPPP is enabled, you need to configure the individual WAN ports. The **WAN 1**, **WAN 2** and **WAN 3** tabs allow you to configure the individual ports for separate use (i.e., non-MLPPP) or in bonded use, as with MLPPP. Select each tab, and enter the identical **User Name**, **Password**, and **Dial Number** for each port.

The screenshot shows the 'MTPSR3_200 - Internet Setup' dialog box with the 'WAN 1' tab selected. The 'Dial Number' field is empty. Under the 'PPP' section, 'Enable' is checked, 'Data Compression' is unchecked, and 'VJC' is checked. In the 'Authentication' section, 'PAP or CHAP' is selected. The 'User Name' and 'Password' fields are empty. The 'Periodic Timer' is set to 5 and the 'Number of Retries' is set to 5. Under the 'SLIP' section, 'Enable' is unchecked and 'Maximum Transmit Unit' is set to 1006. The 'CSLIP (Van Jacobson Compression)' checkbox is also unchecked. 'OK', 'Cancel', and 'Help' buttons are at the bottom right.

Once this is done, click **OK** and you will be returned to the Proxy Setup dialog box.

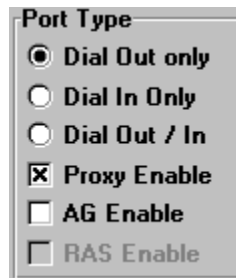
Enabling MLPPP also affects the **WAN Setup** dialog. If you click the WAN button, you will notice that the **Port Type** group has been set to **Dial Out Only** and **Proxy Enable**.

The screenshot shows the 'MTPSR3_200 - WAN Setup' dialog box with the 'WAN 1' tab selected. Under the 'Port Enable' section, 'Port Enable' is checked, 'Script Enable' is unchecked, and 'Restart Script On Communication Failure' is unchecked. In the 'Mode' section, 'Asynchronous' is selected. 'Baud rate' is set to 115200 and 'Clock' is set to 4800. 'Send Idle Flags' is checked. Under the 'Connection Method' section, 'Direct Connect / Leased Line' is selected. The 'Modem Types' dropdown is set to 'Multi-Tech 56K Lucent Socket Modem'. In the 'Port Type' section, 'Dial Out only' is selected. 'Proxy Enable' is checked, while 'AG Enable' and 'RAS Enable' are unchecked. Under the 'Link Usage Control' section, 'Enable' is checked and 'Idle Time' is set to 10 minutes. There are fields for 'active connections' (set to 0) and 'active IP host machines'. A list for 'Hosts restricted only to this port' is empty, with 'Add' and 'Delete' buttons. At the bottom, the 'Asynchronous Gateway' section shows 'General Name' as 'MODEM1', 'Specific Name' as 'LINE1', and 'Port Idle Time' as 20. 'OK', 'Cancel', 'Help', and 'Script' buttons are at the bottom right.

The rest of the Port Type options are inactive (grayed-out). When MLPPP is disabled, all the Port Type options become active again.

Port Type

The Port Type group (in the WAN Setup dialog) is used to configure the ports for specific applications. The default settings for this group are **Dial Out only** and **Proxy Enable**.



This default setting works if you are setting up the WAN port to communicate with the Internet. If this is the case, the WAN port must be enabled and the Port Type group configured for **Dial Out Only** or **Dial Out/In** and the **Proxy Enable** option selected. As mentioned earlier, the **Internet Setup** dialog box is used to configure the Internet Link Control Protocol, i.e., call connection and handshaking.

The Asynchronous Gateway (**AG Enable**) feature can be used on WAN ports configured as **Dial Out only** or **Dial Out/In**. This feature is used to enable the ProxyServer to have a port available for a remote user running a communications package to gain access to an available port on the ProxyServer and dial out. When you enable this feature the **Asynchronous Gateway** group (at the bottom of the dialog) becomes active. Refer to the on-line Helps for a description of features in this group.

The WAN ports can also be configured for remote access (**RAS Enable**) with either the **Dial In Only** or **Dial Out/In** option enabled. If enabled, you must enable **Remote Access** and enter the WAN port IP address in the **IP Setup** dialog box. This ensures that the selected WAN port and the Remote Address assigned to it are in the same LAN segment. The remote IP address is assigned to the remote user.

Changing Internet Parameters

The **Internet Setup** dialog box displays the phone number the ProxyServer is going to dial to reach your ISP, the protocol the ISP supports, MultiLink Point-to-Point Protocol (MLPPP) option, and if you would link the ProxyServer to dial a telephone when you power on your unit.

The screenshot shows the 'MTPSR3_200 - Internet Setup' dialog box with the 'WAN 1' tab selected. The 'Dial Number' field is empty. Under the 'PPP' section, 'Enable' is checked, 'Data Compression' is unchecked, and 'VJC' is checked. The 'Authentication' section has 'PAP or CHAP' selected. The 'User Name' and 'Password' fields are empty. The 'Periodic Timer' is set to 5 and the 'Number of Retries' is set to 5. Under the 'SLIP' section, 'Enable' is unchecked, 'Maximum Transmit Unit' is set to 1006, and 'CSLIP (Van Jacobson Compression)' is unchecked. There are 'OK', 'Cancel', and 'Help' buttons on the right.

The **Dial Number** field displays the phone number of the ISP you initially assigned during your initial configuration. If you have the MLPPP option enabled in Advanced, then the ISP telephone number has to be same for each WAN port connected to the ISP. If a WAN port is not being used for Internet access, then the Dial Number field should be blank.

ProxyServer supports Point-to-Point Protocol (PPP) and Serial Line Internet Protocol (SLIP) on its WAN links. The majority of the time the ISP is going to support PPP. PPP supports two user authentication protocols; Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP). When you established your Internet account your ISP should have indicated which protocol it supports.

Your user name and password are displayed in the PPP group for those WAN ports that are going to be connected to the Internet. The user name and password were entered in the Default WAN Link(s) setup dialog box during the initial configuration. If a WAN port is not being used for Internet access, then the User Name and Password fields will be blank. You can change your User Name and Password in these fields for the selected WAN port. Remember that if you change one of your user names or password and you have the MLPPP option enabled, you must change your user name and password for each WAN port connected to the Internet.

Clicking the **Advanced** tab brings up the parameters that affect all of the WAN links.

The screenshot shows the 'MTPSR3_200 - Internet Setup' dialog box with the 'Advanced' tab selected. The 'Message Printing Control' section has 'Printing', 'LCP', 'Alarm', and 'NCP' all unchecked. The 'Echo Request' section has 'Maximum Number' set to 6 and 'Send Interval' set to 0. The 'Termination Request' section has 'Maximum Number' set to 10 and 'Send Interval Max' set to 5. The 'MultiLink PPP (MLPPP)' section has 'Need to dial out initially' checked. The 'Configuration Requests' section has 'Maximum Number' set to 6, 'Send Interval Max' set to 5, and 'Backoff Interval' set to 10. There are 'OK', 'Cancel', and 'Help' buttons on the right.

The **Message Printing Control** group is used to flag specific items for generating messages on various conditions, including Printing, Alarm, NCP (NetWare Core Protocol), and LCP (Link Control

Protocol) messages. These messages can be useful as troubleshooting tools; however, it is recommended that under normal circumstances all items should be disabled to avoid degradation of ProxyServer performance.

The ProxyServer is capable of performing MultiLink Point-to-Point Protocol (MLPPP). MLPPP provides the opportunity for greater bandwidth by bundling WAN port links. Check **MultiLink PPP (MLPPP)** to enable this option if your ISP provides this support.

Note: In order for link bundling to take place, you need to make sure that the User Names and Passwords of all the WAN port links are identical. Verify and/or change using the individual WAN tabs.

If the **Need to dial out initially** option is enabled (the default) the ProxyServer will (at startup) dial the phone number entered in the Dial Number window. If this option is disabled, then the ProxyServer will not dial out until it receives a request to dial out.

The **Echo Request** group allows you to configure the Link Control Protocol (LCP) Echo Request parameters. Options include Maximum Number of unacknowledged LCP Echo requests allowed before triggering the termination of the link to the peer (valid range is 1 to 20 with a default of 6 requests) and Send Interval defines the interval that the LCP will insert between two consecutive LCP Echo Requests (valid range is 0 to 65535 with a default of 0 seconds).

The **Termination Request** group allows you to configure the Link Control Protocol (LCP) Termination Request parameters. Options include Maximum Number of LCP Termination Requests issued after the completion of a back-off interval (valid range is 1 to 20 with a default of 10 requests); and, Send Interval Max defining the interval that the LCP will insert between two consecutive LCP Termination Requests (valid range is 5 to 65535 with a default of 5 seconds).

The **Configurations Requests** group allows you to configure the Link Control Protocol (LCP) Configuration Request parameters. Options include Maximum Number of requests to be sent before backing off due to no response (valid range is 3 to 65535 with a default setting of 6 requests); Send Interval Max defining the interval between two consecutive LCP configuration requests (valid range is 5 to 65535 with a default of 5 seconds); and, Backoff Interval defining the interval that the LCP will insert once the unanswered Maximum Number of Configuration requests has been reached (valid range is 5 to 65535 with a default of 5 seconds).

Enabling the DHCP Server

The Multi-Tech DHCP (Dynamic Host Configuration Protocol) server feature manages all IP address assignments within a local/private LAN. The DHCP Server maintains a list of available IP addresses and when a client computer asks for one, the DHCP Server sends the IP Address to the client. The client computer, configured with that information, can then participate in the TCP/IP network.

What are the advantages of DHCP? Why not let your systems administrator assign permanent IP addresses? Because DHCP assigns IP addresses only to computers that are active on a TCP/IP network, non-active computers do not need to reserve an IP address. This helps workgroups that have limited numbers of IP addresses. DHCP also simplifies the process of setting up clients. Instead of having to remember which IP addresses you've assigned and which addresses are free, you can simply configure the client for DHCP and let the DHCP server do the rest (Refer to Chapter 5 - Client Setup).

To display the **DHCP Server Setup** dialog box, click the **DHCP Server** button on the **Proxy Setup** menu. To enable the DHCP Server, click (check) the **Enable** option and make appropriate choices.

The **DHCP Server Setup** menu allows you to customize each client PC configuration from one central point. The **Manage Addresses** group allows you to establish the range of IP addresses for the workgroup (From - To). You can then exclude specific addresses from that range in the **Exclude Range** field. Excluded addresses (individual IP addresses or a range of addresses) are computers with static IP addresses (e.g., a DNS server, a WINS server, and the DHCP server itself). You can also add, delete, edit, and bind addresses using the corresponding buttons in this group.

The **Option Types and Values** group at the bottom of the dialog box allows you to customize the configuration of the client platform. You can add, delete, and edit an option by highlighting it and clicking the appropriate button. You cannot, however, edit or delete entries provided in the default list.

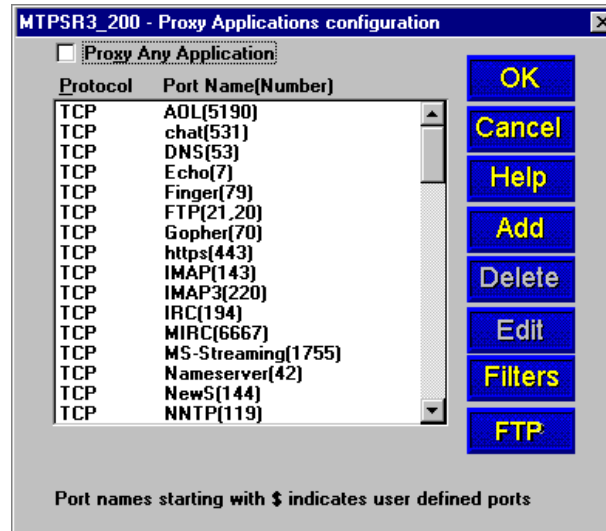
This group includes the Router Address which is the location on the IP subnet that a client can use; the Domain Name which is the human-readable Internet name of your IP domain; the Reassembly size which sets a maximum datagram reassembly size; the Default IP TTL which sets the IP time-to-live limit (max. 255); the MTU (Maximum Transmit Unit) which sets the largest possible unit of data that can be sent; the Default TCP TTL which sets the TCP time-to-live limit; and the Lease time option which sets the time duration that an IP address is assigned to a client.

When a client requests an IP address, it is given that address for a specific duration of time. Once the time duration has expired, the client must have received an extension on the lease or received another IP address to use. The default lease is 65535 seconds (18.2 hours). Assigning lease time depends on your goals and the site's usage patterns. For example, if you have more users than IP addresses, a shorter lease (hours) would be appropriate; however, if students at a university have their computers turned off for a long period of time (and you want them to keep their IP addresses), then a longer lease (weeks) would be appropriate.

Adding ProxyServer Applications

The **Proxy Applications configuration** dialog box allows the ProxyServer systems administrator to configure the set of applications available for proxying by the ProxyServer.

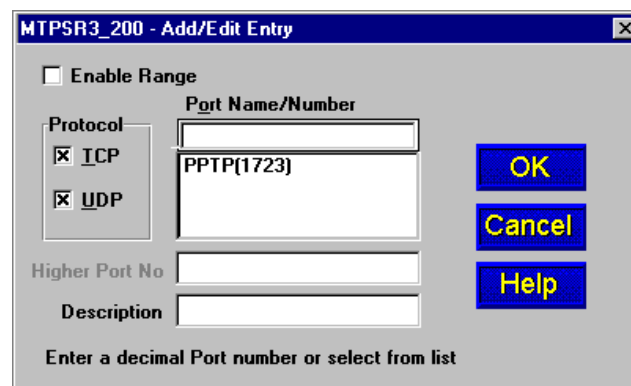
Click the **ProxyServer** button in the **Proxy Setup** menu to display the **Proxy Applications configuration** dialog box which lists all the applications currently supported by the ProxyServer. This list includes many of the most common port usages; however, not all are included because an increase in the number of port usages supported means a *possible* decrease in performance speed and an increased security risk.



Use the **Add/Edit Entry** dialog box to add or edit ProxyServer applications. For procedural details, refer to the ProxyServer **Help**.

The option to add ProxyServer applications is important as new software programs are continually being developed to perform useful tasks. For example, you may want to add new database managers, spreadsheets, communications packages, graphics programs, etc., anything that would make your job easier.

Editing considerations might mean enabling/disabling protocols (both TCP and UDP are enabled by default), changing the ProxyServer description (to be more easily identified), or changing the range of port numbers to exclude/include other users (refer to the ProxyServer **Help** for details).



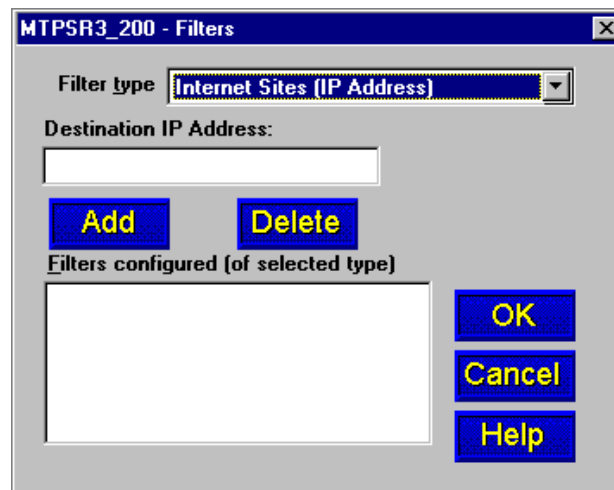
You must first determine which currently unsupported applications can be proxied. You can refer to RFC 1700 on the Internet which defines the Internet Protocol suite. RFC 1700 identifies the parameters, such as Internet address, domain names, autonomous system numbers, protocol numbers, port numbers, and many others. Once the necessary information has been determined, you can add the application(s) to the supported list. Without this information, the Proxy will not allow packets through to the Internet from the unknown software.

The ProxyServer administrator can set up “filters” on the proxy server for better control. The **Filter** option can be used when you want to block all packets originating from a specific destination (called source address filtering) or all packets heading for a particular destination (called destination address filtering). Filters can be set to exclude packets of a particular protocol or any particular field in a LAN packet.

These filters are based on three basic filter types: **Internet Sites (IP Address)** (both dotted decimal and Domain Name), **Client Workstation** (MAC address or IP address), or **Application**. To install a filter, you must first choose one of these basic filter types. Refer to the ProxyServer **Help** for details on how to configure the **Filter** option.

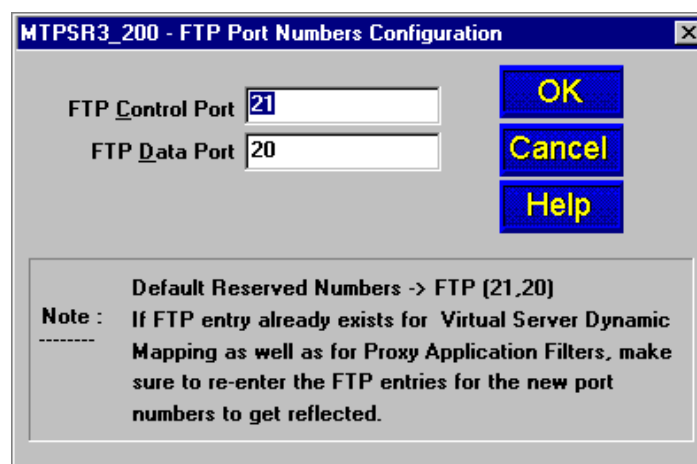
For example, in a filter set up by Domain Name, the system administrator could restrict all users at a particular site from accessing game sites, X-rated sites, etcetera; or, users at a particular MAC address or IP address could be restricted from using the services of the ProxyServer; or, you could restrict all users from accessing specific applications (e.g., FTP, chat, etcetera).

Note: The **Filter** option does not perform content filtering; rather, the system administrator needs to restrict users from the particular Internet site, client workstation, or application through the **Filters** dialog box.



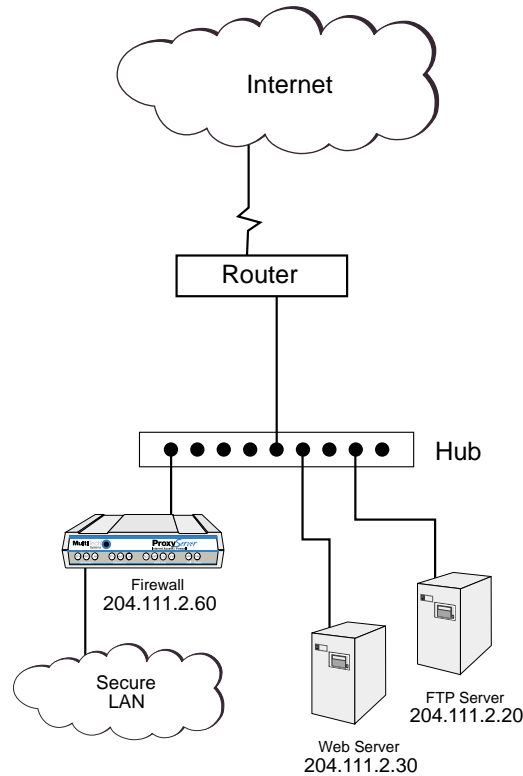
Note: Adding applications may decrease performance speed and increase security risks. Therefore, you may want to delete unused or rarely used applications.

To further enhance the security of the firewall network, the **FTP** button on the **Proxy Applications Configuration** dialog box allows you to change the FTP Control Port and Data Port Numbers. If you do change these numbers, make certain that you inform users who need to access the FTP server what the new numbers are. By default, the FTP server's Control Port Number is 21 and the Data Port Number is 20.



Enabling the Virtual Server

The virtual server feature of the ProxyServer allows you to have multiple servers on your local area network (LAN) with one static IP address (from your ISP or Multi-Tech's Global Dynamic WAN Addressing) assigned to each WAN port. A normal internet connection requires a static IP address for each server on your LAN. A normal Internet connection is shown in the following illustration.

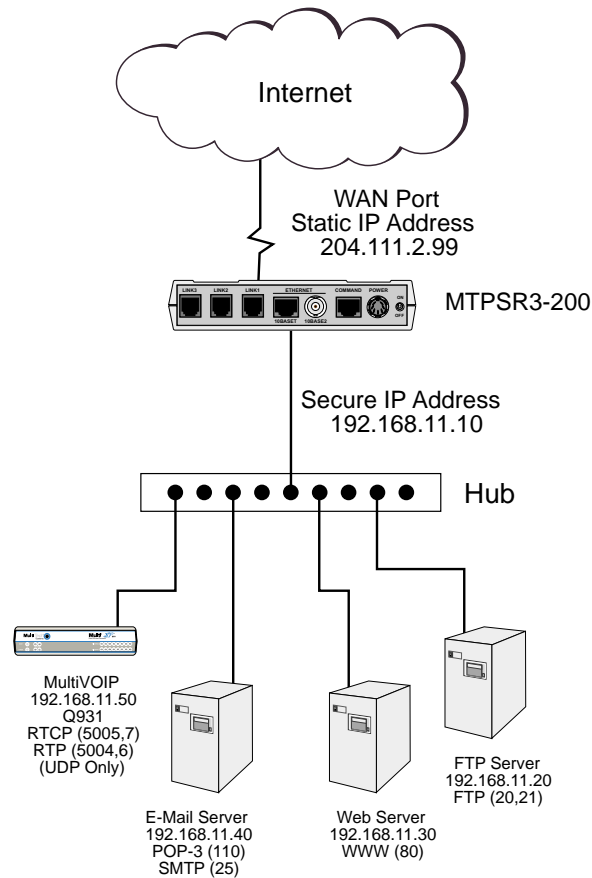


In a normal Internet connection with a router connected to the Internet, you need a static IP address for each function (server) you want to perform on the Internet. For example, to have a Web server browse the internet for you, you need an IP address so that the router knows where the traffic is coming from and where to send the reply. In our normal Internet connection we have assigned an address of 204.111.2.30 for the Web server, address 204.111.2.20 for the FTP server, and 204.111.2.60 for the Firewall.

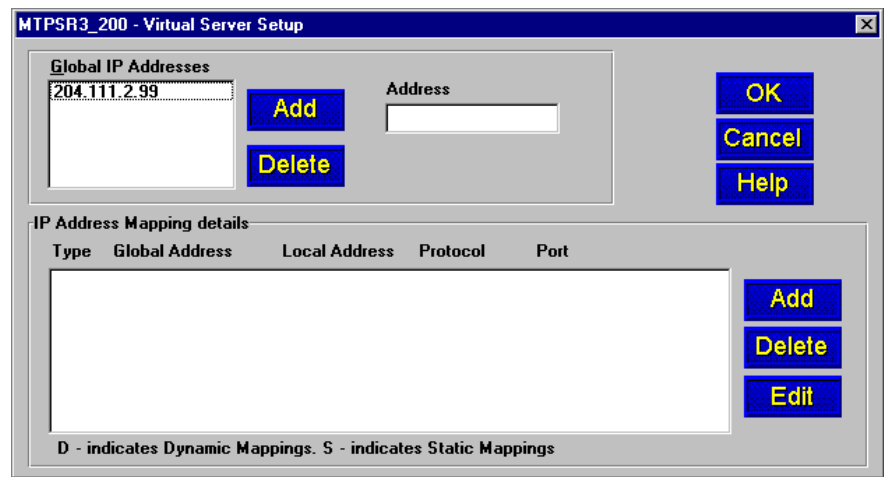
To reduce the number of static IP addresses, a virtual server feature is present in the ProxyServer that allows you to map multiple local servers to a single static IP address or to a Global Dynamic WAN port address. The virtual server feature enables the ProxyServer to take requests from different servers (functions) and interact with the Internet based on the functionality of the request. In the normal Internet connection, this was a physical linkage to a specific IP address. The virtual server feature is a functional connection. Functionality is defined by how the server is used; i.e., the Web server uses a www-http protocol, an e-mail server uses pop-3 and SMTP protocol. Therefore, multiple requests can be sent to the Internet over a single physical connection and the ProxyServer will know which server is requesting service. The following illustration shows how a ProxyServer is connected to the Internet with a single static IP address or Global Dynamic WAN port address and the same servers used in the normal Internet connection are now connected to the Internet through the ProxyServer.

Now, if instead of mapping a static IP address from your ISP to the ProxyServer, you employed Multi-Tech's Global Dynamic WAN port addressing method, you no longer have to be concerned with a single static IP address from your ISP. You can assign a predefined Global Dynamic WAN port

address to each of the ProxyServer's WAN ports and then map your servers to that WAN port address the same way you would map a static IP address from your ISP. The predefined Global Dynamic WAN port addressing scheme is 0.0.0.1 for WAN port 1, address 0.0.0.2 for WAN port 2, and 0.0.0.3 for WAN port 3. If MLPPP is being used, you can assign 0.0.0.0 to all three WAN ports. You can dynamically map any one Global Dynamic address to any WAN port on the ProxyServer and statically map the other two ports, or you can statically map all three WAN ports.

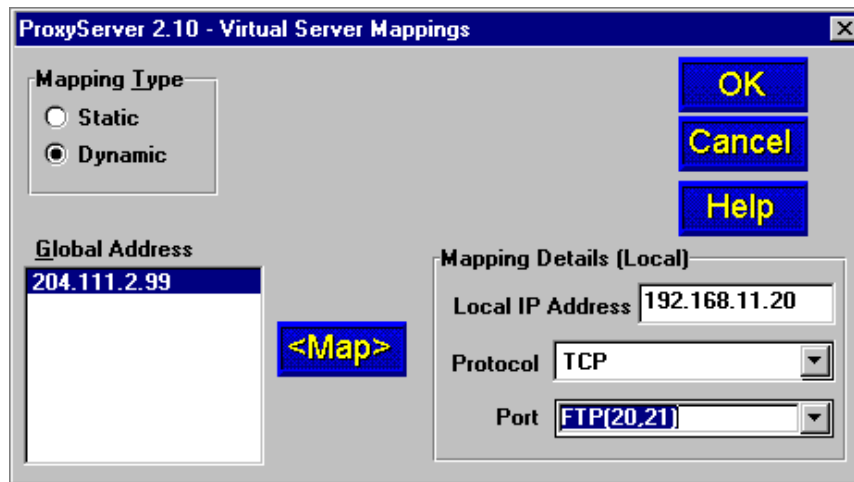


The **Virtual Server Setup** dialog box defines how the servers are connected to the one global IP address. The static IP address that we established in our virtual server connection example above is added to the Global IP Addresses group in the Virtual Server setup dialog box. This could also be a Global Dynamic WAN address.



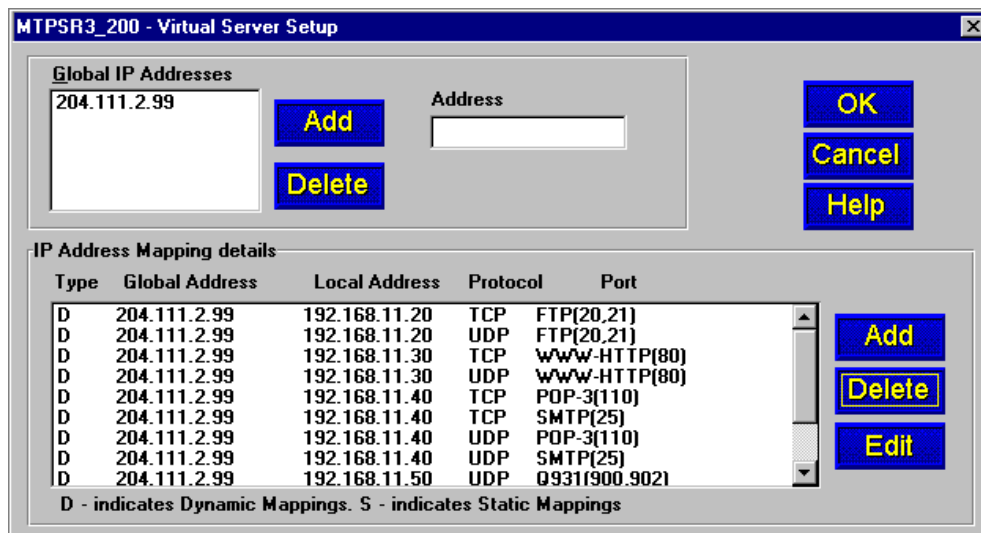
With static IP addressing, the Global Ip Address is the IP address that is seen by the Internet. This global address will be used by the virtual server feature to filter the activity of the traffic to and from

the Internet by functionality. The addresses that we assigned to our servers in the virtual server example are unregistered addresses that are only seen by the ProxyServer. These local IP addresses are arbitrarily assigned to servers in our virtual server connection example. For example, we assigned IP address of 192.168.11.20 to the FTP server, 192.168.11.30 to the Web server, 192.168.11.40 to the e-mail server, and 192.168.11.50 to the MultiVOIP.



These local addresses are then mapped to the global address by function. The FTP server was assigned an IP address of 192.168.11.20 with a TCP and UDP protocol and a port number of 20 and 21. The Mapping Details [Local] group in the Virtual Server Mappings dialog contains the FTP server local mapping information. When the FTP server mapping information is entered, the Web server can be mapped to the global address by entering the IP address 192.168.11.30 in the Local IP Address field of the Mapping Details [Local] group with its protocol and port information. Then the mail server, and if a MultiVOIP is used in the local network - its mapping information, can be added to the local mapping group.

The Virtual Server Setup dialog displays all the local mapping information.



Enabling Remote Servers

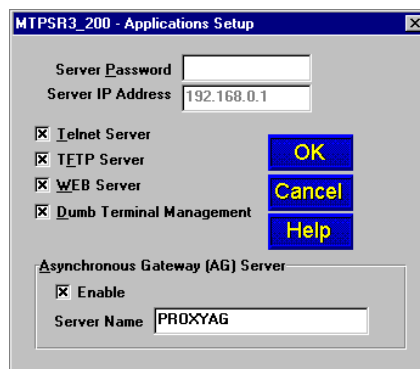
The **Applications Setup** dialog box lets you set up support for Telnet Server, TFTP (Trivial File Transfer Protocol), WEB Server, and Dumb Terminal Management in the ProxyServer.

Telnet/TFTP

Telnet is an applications level protocol commonly found in IP-based networks that allows terminal emulation at a remote workstation. To do this, there is usually a server at a central point that allows multiple clients to connect and request to use the service. The service could be anything. Usually it is terminal emulation. The ProxyServer has a Telnet server that allows multiple clients to connect and request to use Telnet service, usually terminal emulation. Telnet is most often implemented over TCP.

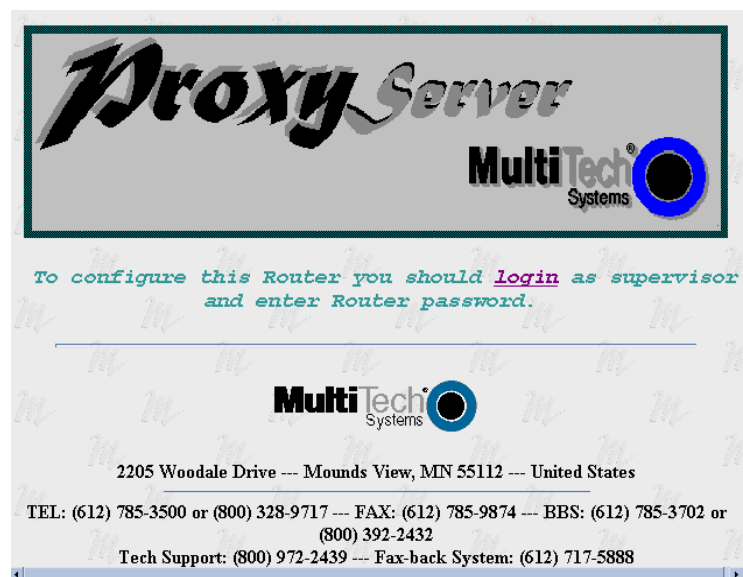
TFTP is a file transfer protocol that uses UDP and provides a simple method for transferring files between two nodes (the server and the client).

To display the **Applications Setup** dialog box, click **Others** on the **Proxy Setup** main menu.



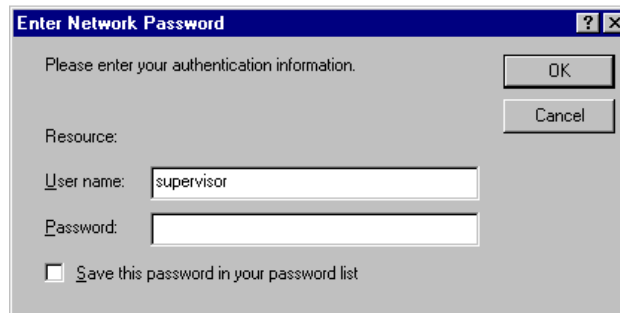
WEB Server

The Web Server interface allows you to configure the ProxyServer remotely through your Web browser on your local network. Enter the IP address of the ProxyServer in the Location (Address) field of your browser to launch the Multi-Tech ProxyServer Configuration site.



By scrolling down the browser scroll bar, you are presented with a link to log in to the ProxyServer configuration menu ("Click Here to Login"), as well as links to Multi-Tech's WWW site, FTP site, and Tech Support site.

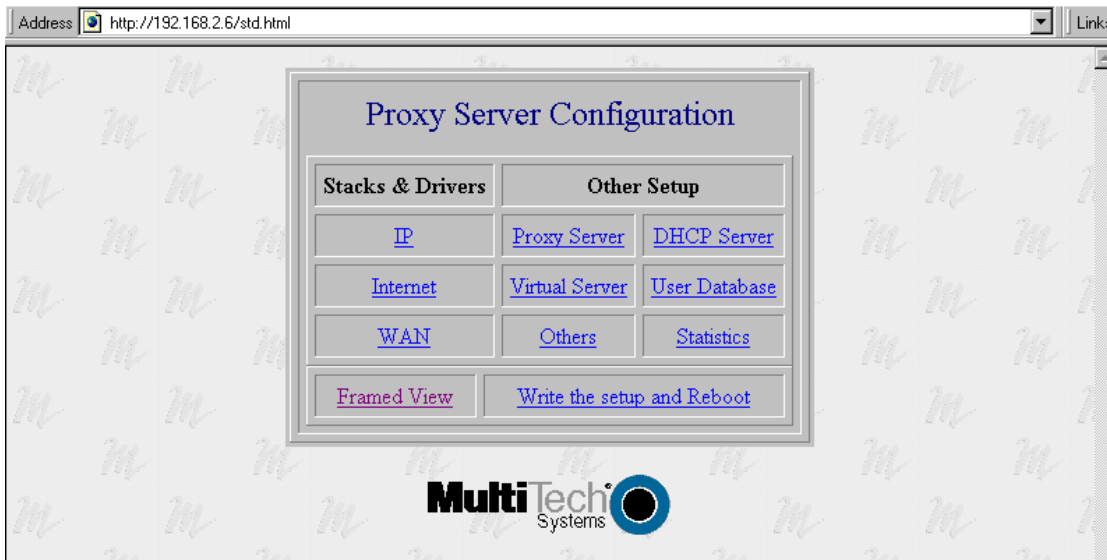
Click the word “**Login**” to launch the ProxyServer Configuration program. The **Enter Network Password** dialog box is displayed.



The dialog box titled "Enter Network Password" has a blue title bar with a question mark and close button. The main area is light gray and contains the text "Please enter your authentication information." in the top right. Below this are two buttons: "OK" and "Cancel". The "Resource:" label is followed by a text field containing "supervisor". Below that is a "Password:" label followed by an empty text field. At the bottom left is a checkbox labeled "Save this password in your password list".

Type the term “supervisor” in the **User Name** field (no password is needed) and click **OK**.

The **Proxy Server Configuration** menu is displayed.

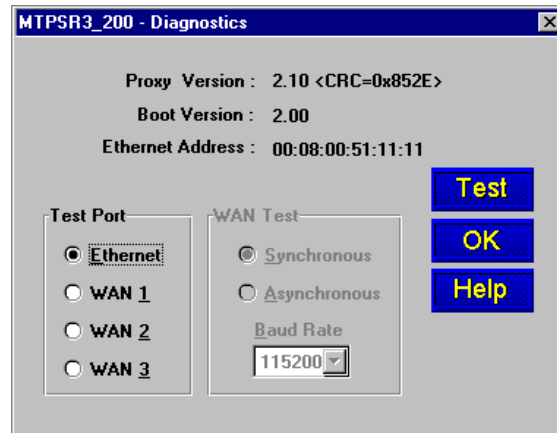


The **Proxy Server Configuration** menu provides several categories: Protocol Stacks, Device Drivers, Other Setup, and Statistics for each of the WAN ports. Each category provides links which allow configuration of various features. Click the item you need to configure and the program displays a configuration dialog box for that feature.

Note: The first user to access the ProxyServer will have *read/write* rights over the unit. All subsequent users will have *read only* rights, and therefore, some of the options within the Web interface will be inactive (i.e., will not be linked).

Running Diagnostics

The ProxyServer Setup program lets you perform various hardware tests on the LAN and WAN links. The **Diagnostics** dialog box is displayed by clicking the **Built in Test** button in the **ProxyServer Setup** dialog box.

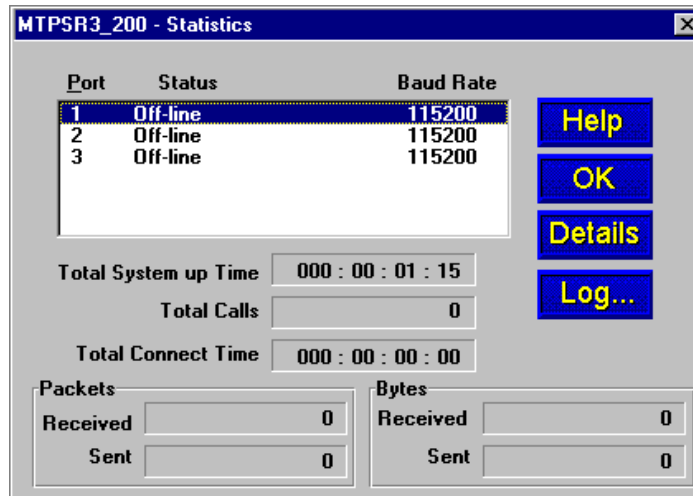


Diagnostic tests are performed if the Communication type of the Local Port configuration is set to COM Port. If the Local Port configuration is set for IP, no diagnostic tests are performed by the ProxyServer.

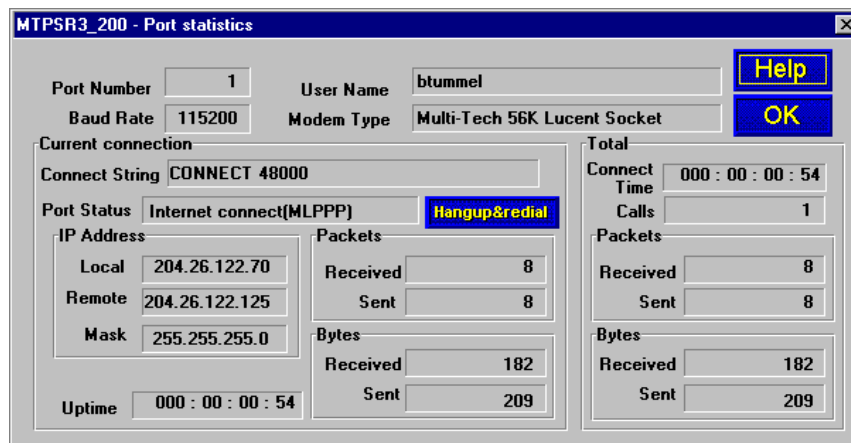
Note: Test will FAIL unless loopback plugs are used on the port you are testing.

Running Statistics

The **Statistics** dialog box allows you to view the real-time WAN statistics for the ProxyServer. This includes a list of the available WAN ports, the state of the attached modems, and the current baud rates. To view details of a specific port, double-click the entry in the Port list or highlight the entry and click Details.



The Port Statistics dialog box provides information relating to the traffic on the ProxyServer's WAN port. These statistics can be helpful in troubleshooting suspected problems at the physical layer; i.e., the WAN port itself, the link device, and any associated cabling.



The Port Number field lists the number of the selected port. All other fields in this dialog box are relevant for that port. The User Name field defines the User Name used to login to the Internet through the selected port. The baud rate and modem type are also displayed.

The Connect String field displays a message (e.g. CONNECT 48000) reported by the modem during connection. The Port Status field displays the current status of the selected port (e.g., Internet connectMLPPP). The IP Address Group displays the parameters of the current connection. The Uptime field indicates the amount of time elapsed since the current connection initiated. The Packets Group displays packet traffic details and the Bytes Group displays the bytes traffic details for the current connection.

The Connect Time field indicates total duration of the connection on the selected port. The Packets Group displays the packet traffic details for the time period the ProxyServer came up and the Bytes Group displays the bytes traffic details for the time period since the ProxyServer came up.



Chapter 5 - Client Setup



Introduction

The information provided in this chapter enables multiple users to configure their PCs to access the Internet through a ProxyServer. The procedures are divided into two sections, based on operating platform. The first section covers configuration of Windows 98/95 PCs, and the second section covers configuration of Windows NT (4.0 Workstation) PCs.

Before you Begin

Before you begin the client setup process, read through the following requirements:

ProxyServer

The ProxyServer was configured by the administrator who, while installing the software, determined that the ProxyServer would either automatically assign Internet (IP) addresses, or require that they be assigned manually to each client PC. Also, the administrator assigned an IP address to the ProxyServer's Ethernet port, and assigned user names and passwords to the WAN links. All these factors play a role in client configuration. Make certain that you are aware of the decisions made prior to setting up client PCs.

PC

To access the ProxyServer, your PC must have communications capability including hardware such as a network card and any necessary software.

If the ProxyServer does not automatically assign an IP address to each PC, you will have to obtain it from your network administrator. You will also need the IP address for the ProxyServer (the Gateway address), and the IP Address of your organization's Domain Name Server (DNS). All these items are needed so your PC can identify the ProxyServer as its gateway and properly set up your network security.

Checklist

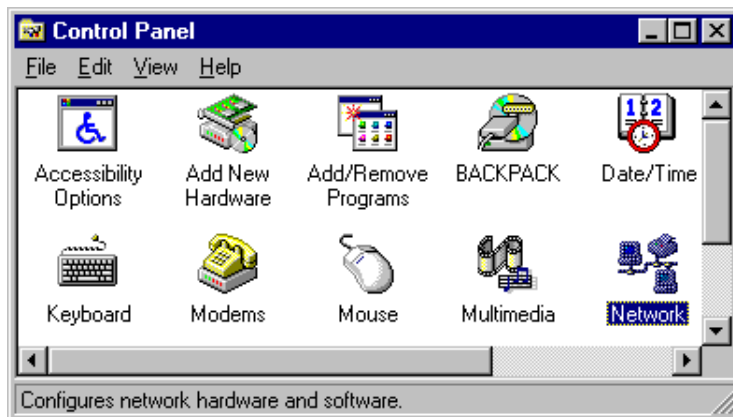
A checklist has been provided towards the end of each procedure (Step 16). This checklist is included in the setup so that you can record all the pertinent information required for the connection between your PC and the ProxyServer. Keep this as a reference for future upgrades.

Configuring in Windows 98/95

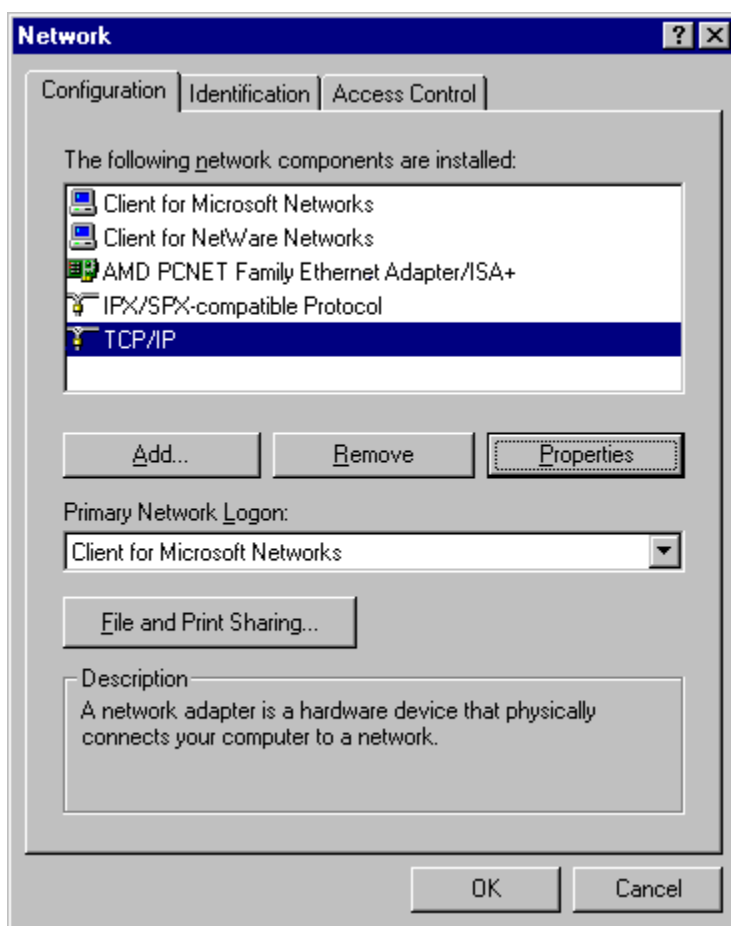
Perform the following steps to set up your Windows 98/95 PC:

Note: All of the hardware and screens used in this section are intended as examples only. Please select options appropriate to your system.

1. Click **Start | Settings | Control Panel** and then double click the **Network** icon.

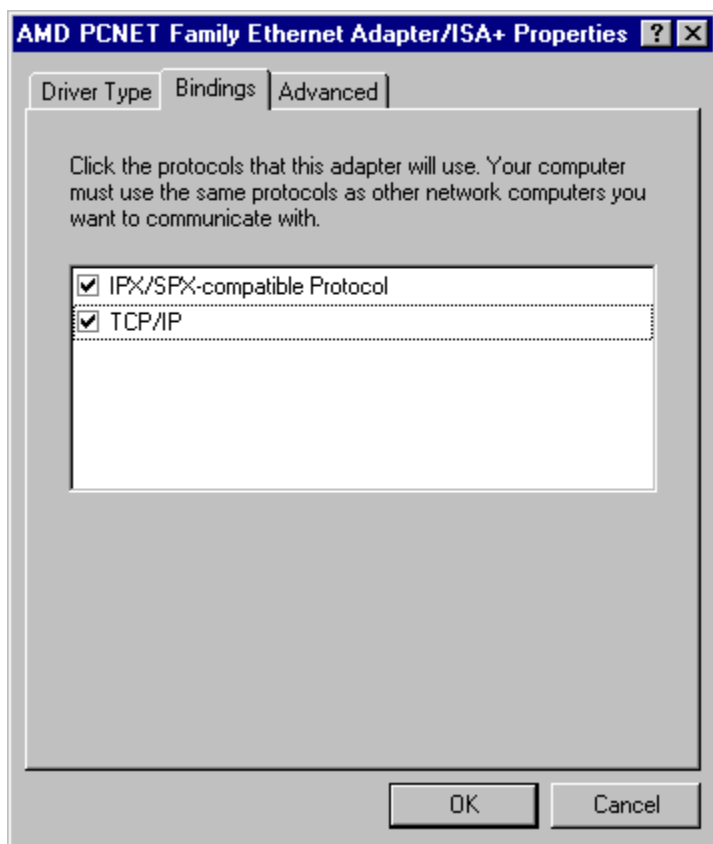


The **Network** dialog box (**Configuration** tab) is displayed which shows all the components (i.e., clients, adapters, protocols, and any services) installed on your PC.



2. If **TCP/IP** is listed, proceed to step 3; otherwise, refer to **Installing TCP/IP (Win98/95)**, at the end of this section.

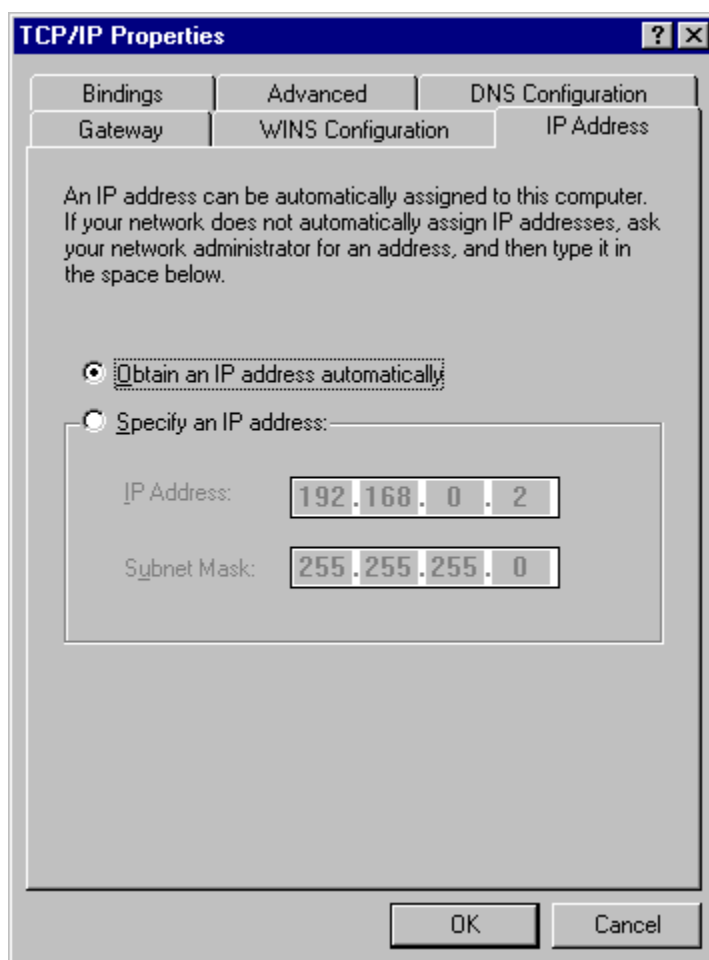
3. Check for binding between the adapter and TCP/IP. In the **Network** dialog box, click your Ethernet adapter to select it, then click **Properties** to display the Adapter Properties window.



4. Click the **Bindings** tab, then if necessary click the box to the left of TCP/IP so this entry is enabled (checked). When you are finished, click **OK** to return to the **Network** dialog box.

Note: There may be other protocols listed and enabled under your Ethernet adapter. This does not affect the TCP/IP protocol. Rather, it simply means your computer will accept messages using those protocols as well as TCP/IP.

5. Select **TCP/IP**, then click **Properties** to open the **TCP/IP Properties** window.



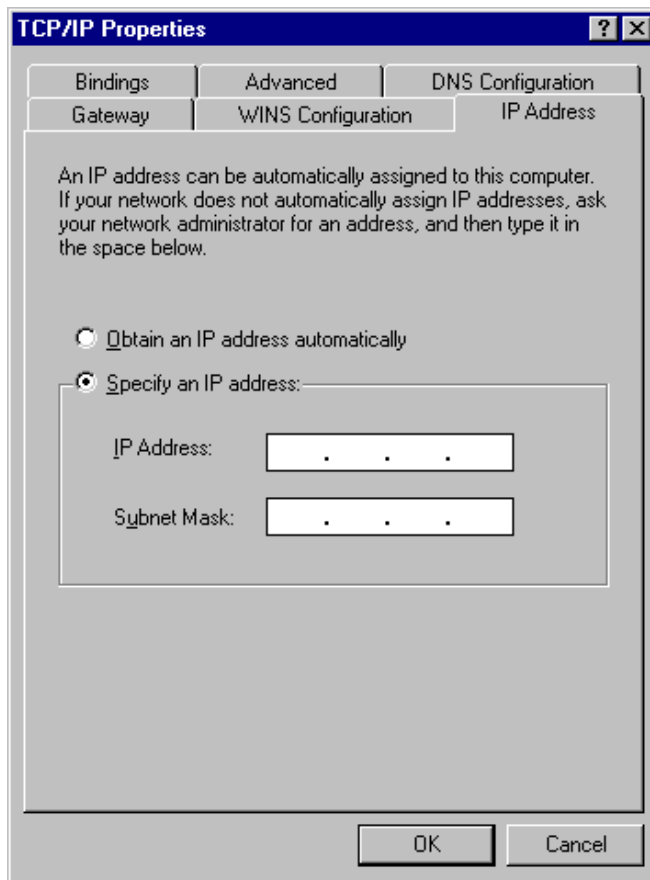
6. Select the **IP Address** tab.

The IP addressing method depends on how your ProxyServer's DHCP Server option was configured. If DHCP Server is active, your IP address is issued automatically. If your network administrator did NOT activate DHCP Services on the ProxyServer, you will have to assign your IP address manually.

Verify the ProxyServer/DHCP status with your network administrator, then proceed to step 7 for DHCP assigned addressing, or to step 8 for manual addressing.

7. If DHCP Services are active on the ProxyServer (default), verify that the **Obtain an IP address automatically** option is selected. You are done; go to step 17 to reboot your PC and attempt to open an Internet session.

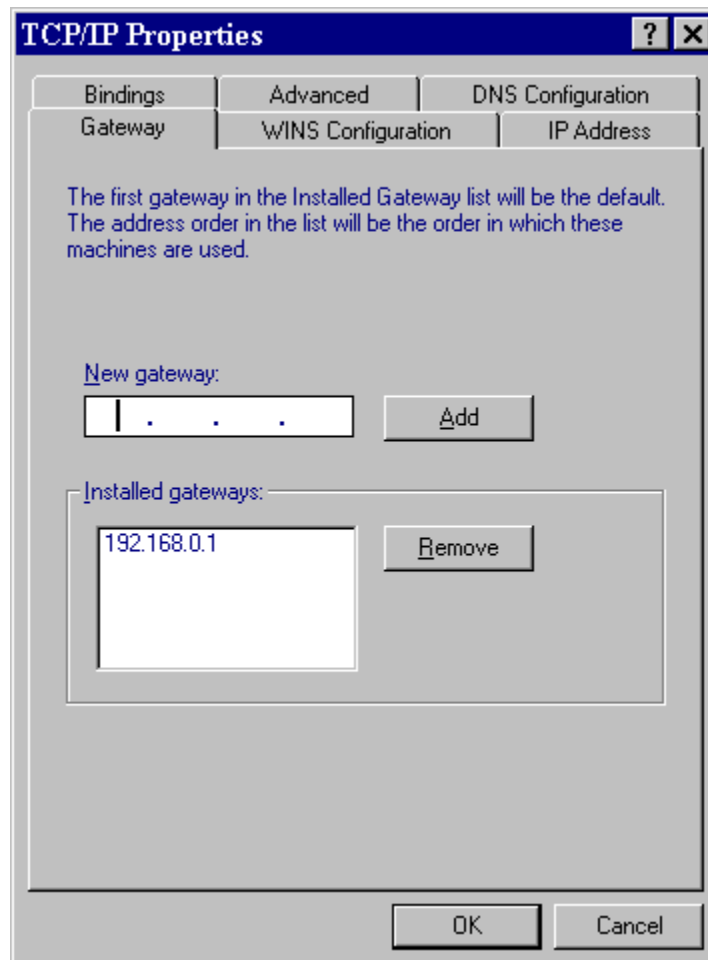
8. If DHCP Services are NOT active on the ProxyServer, you will have to manually enter your IP address. Select manual addressing by clicking the **Specify an IP address** option. The IP Address and Subnet Mask fields become active.



9. In the **IP Address** field, type the IP address assigned to your PC.

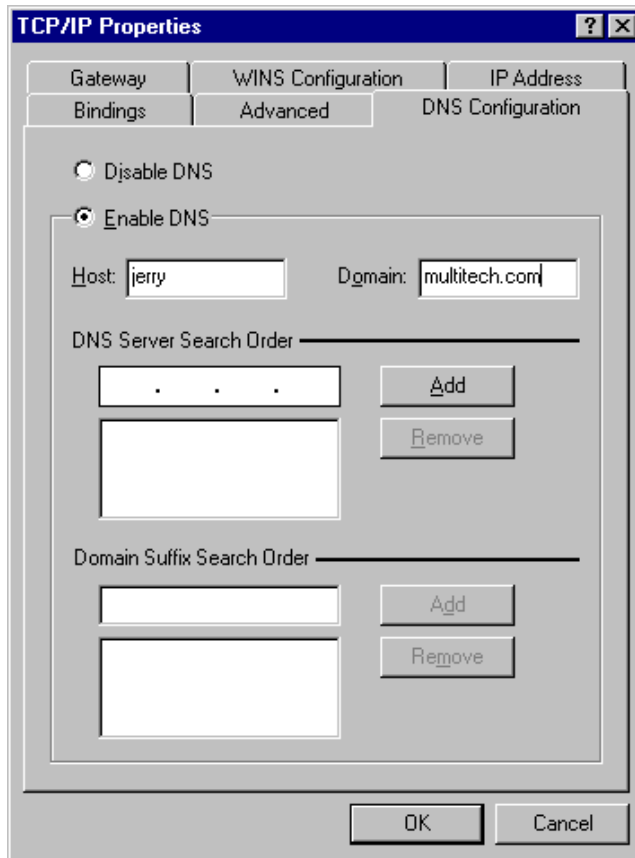
Remove the default IP address (if any) and begin typing the new address. This address is entered in dotted decimal notation and is comprised of four groups (octets) separated by periods or "dots." If a group has fewer than 3 digits, type the necessary digits and press the space bar to move to the next group. When you are finished, verify that the IP address is identical to the IP address you were given for your PC.

10. Click the **Gateway** tab.



11. In the **New gateway** field, enter the IP address of the ProxyServer's Ethernet port and click **Add**. The new gateway address is displayed in the list of **Installed gateways**.

12. Click the **DNS Configuration** tab. Verify that **Enable DNS** is selected (checked).



13. In the **Host** field, enter your user name (i.e., jerry).
14. In the **Domain** field, enter your company's domain name (usually the company name followed by one of the following extensions: .com, .edu, .gov, .org, .mil, or .net. For example, multitech.com).
15. In the **DNS Server Search Order** group, place the cursor in the first group of the address field and type the IP address of your LAN's DNS server (provided by your network administrator). Click **Add** and the new address is displayed in the list below the address field.

Your network may have more than one DNS server, allowing you to use a secondary DNS server if the primary DNS server is not available. If this is the case, add the IP address of the secondary DNS server using the same procedure as with the first.

Note: The address that is displayed first (at the top) of the list is the primary server (the first one searched). You can "drag and drop" the items in the list, if necessary, until the primary DNS server is listed first.

When this is done, click **OK**. You are returned to the **Network** dialog.

16. In the Network dialog, Click **OK**. You are returned to the **Control Panel**.

Use the following checklist to record all the configuration settings for future use:

Configuration Checklist	
IP Address (PC)	. . .
IP Address (ProxyServer)	. . .
Host (User Name)	
Domain	
DNS Server Address	. . .
Network Adapter (Manufacturer/Model Number)	

17. Reboot the PC for changes to take effect.

At this point your client setup is complete. Test your setup by following steps 18 and 19. If you encounter problems, contact your administrator.

18. Initiate an Internet session by double-clicking on your browser icon, or try to FTP a file.

Note: The ProxyServer operates transparently, so there should not be a need for any special proxy settings on your IP applications (i.e., browser, Telnet, or FTP). Set up each application as “No Proxy” or equivalent; or, connect to the Internet over the LAN.

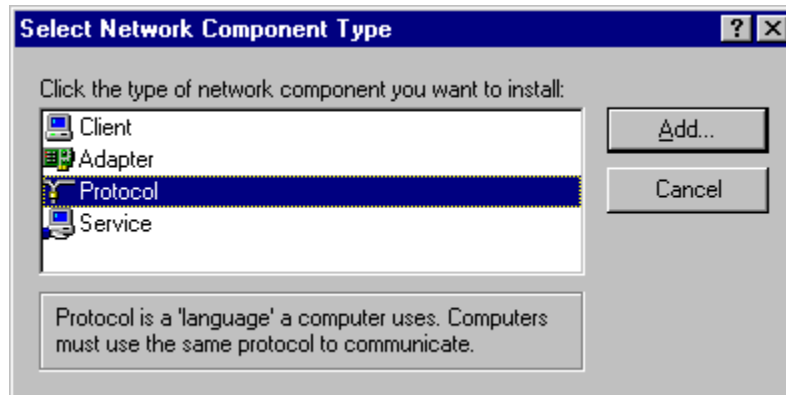
19. To further validate your connection to the ProxyServer, “Ping” the IP address of the ProxyServer.

Installing TCP/IP (Win98/95)

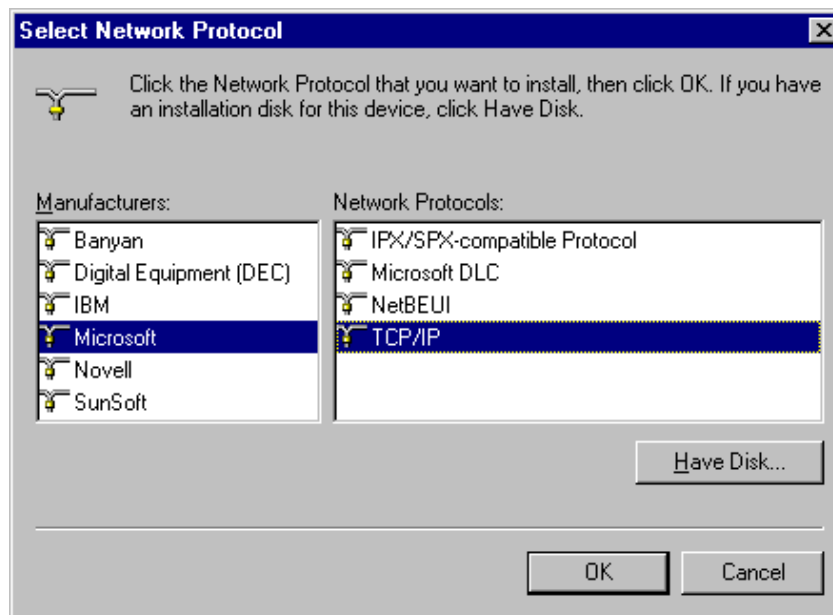
If TCP/IP is not already installed, perform the following steps:

Note: For this procedure you may need your Windows installation disks or CD ROM.

1. In the **Network** dialog box, click **Add**. The **Select Network Component Type** dialog is displayed with a list of installation options.



2. Select **Protocol** and click **Add**. The **Select Network Protocol** dialog box is displayed with protocol options.



3. In the **Manufacturers** list click the manufacturer option (Microsoft in the example) to highlight it. A list of available protocols will appear in the **Network Protocols** list.
4. In the **Network Protocols** list, select **TCP/IP** and click **OK**.
5. Exit the add option. Click the **OK** button.

Note: If Windows does not find the necessary files on the hard drive, click **Have Disk** and follow the on-screen instructions for loading TCP/IP from the installation disks/CD-ROM.

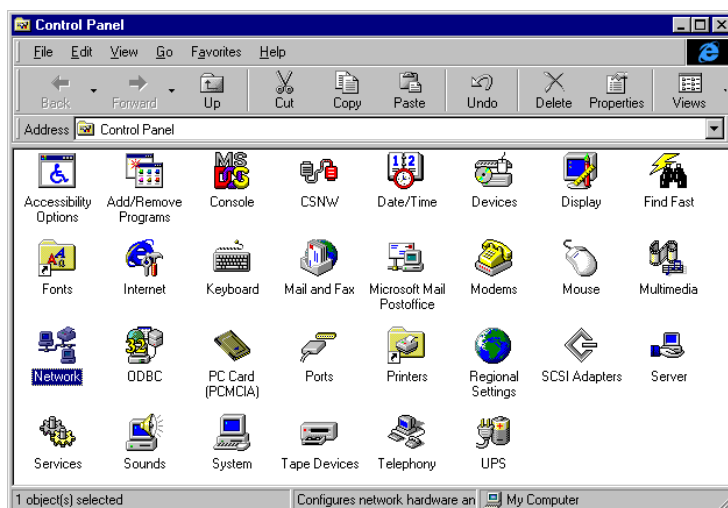
6. Reboot your PC for changes to take effect.
7. Click **Start | Settings | Control Panel** and double-click the **Network** icon to return to the Network dialog. Return to step 3 of the **Configuring in Windows 98/95** and continue with the client setup procedure.

Configuring in Windows NT

Perform the following steps to set up your Windows NT workstation PC:

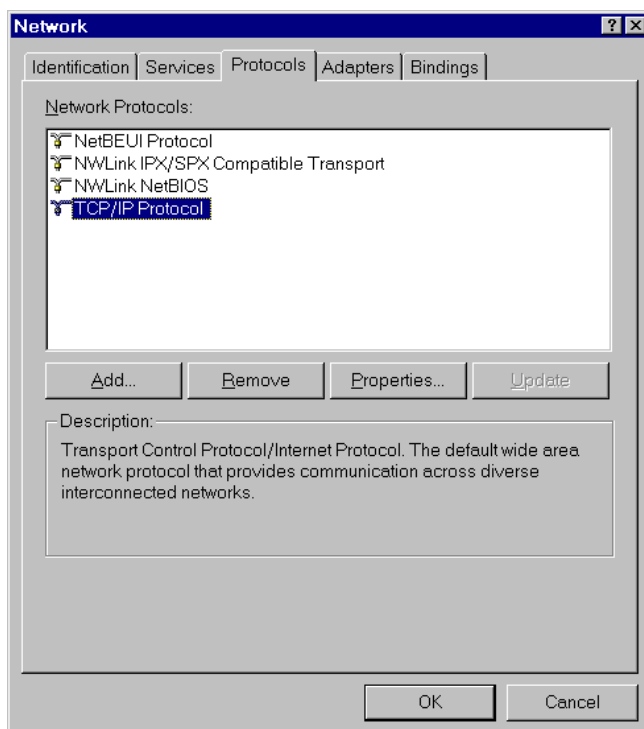
Note: All of the hardware and screen samples in this section are intended as examples only. Please select options appropriate to your network.

1. Click **Start | Settings | Control Panel**.



Double click the **Network** icon.

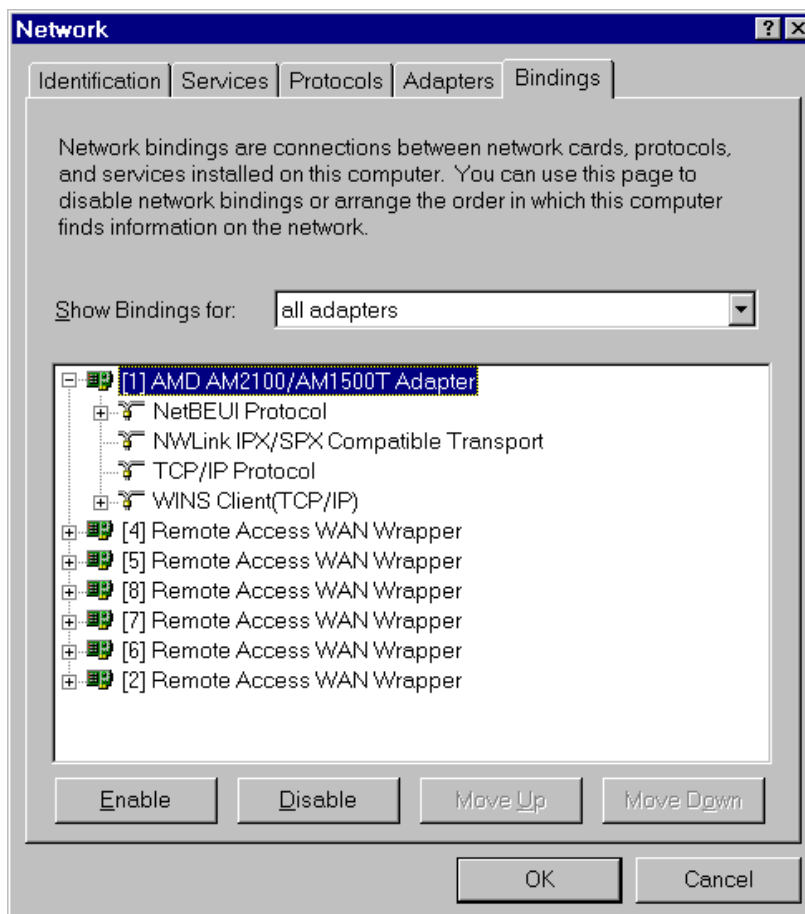
2. The **Network** dialog box is displayed. Click the **Protocols** tab.



A list of protocols currently present on your PC is displayed. Check the installed protocols. If you find **TCP/IP Protocol** listed, proceed to step 4. If TCP/IP is not listed, you must install it prior to proceeding. Refer to **Installing TCP/IP (WinNT)** at the end of this section.

Click the **Bindings** tab.

3. The **Bindings** tab is displayed.

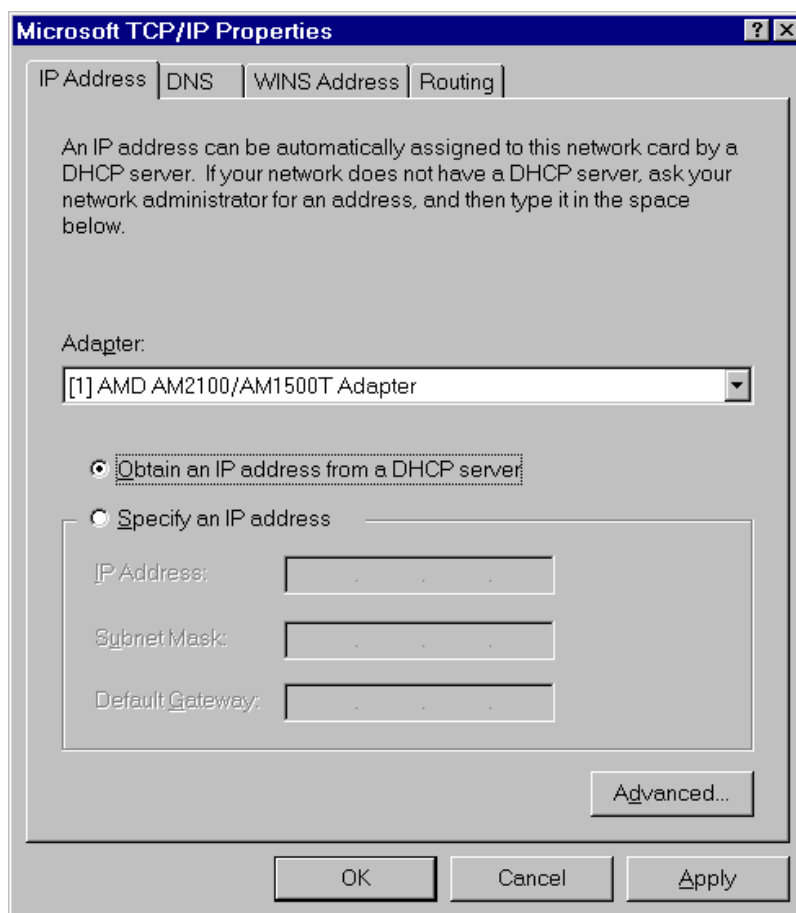


4. In the **Show Bindings for** drop down list, select **all adapters**. A list of all adapters is displayed.
5. Double click the entry for your Ethernet card adapter to expand the list of bindings. Verify that **TCP/IP Protocol** is included in the bindings below your adapter.

Note: There may be other protocols in the list under your Ethernet adapter. This does not affect the TCP/IP protocol. Rather, it simply means your computer will accept messages using those protocols as well as TCP/IP.

6. Click the **Protocols** tab.

7. In the **Network Protocols** list select **TCP/IP**, then click **Properties**. The **Microsoft TCP/IP Properties** dialog is displayed.



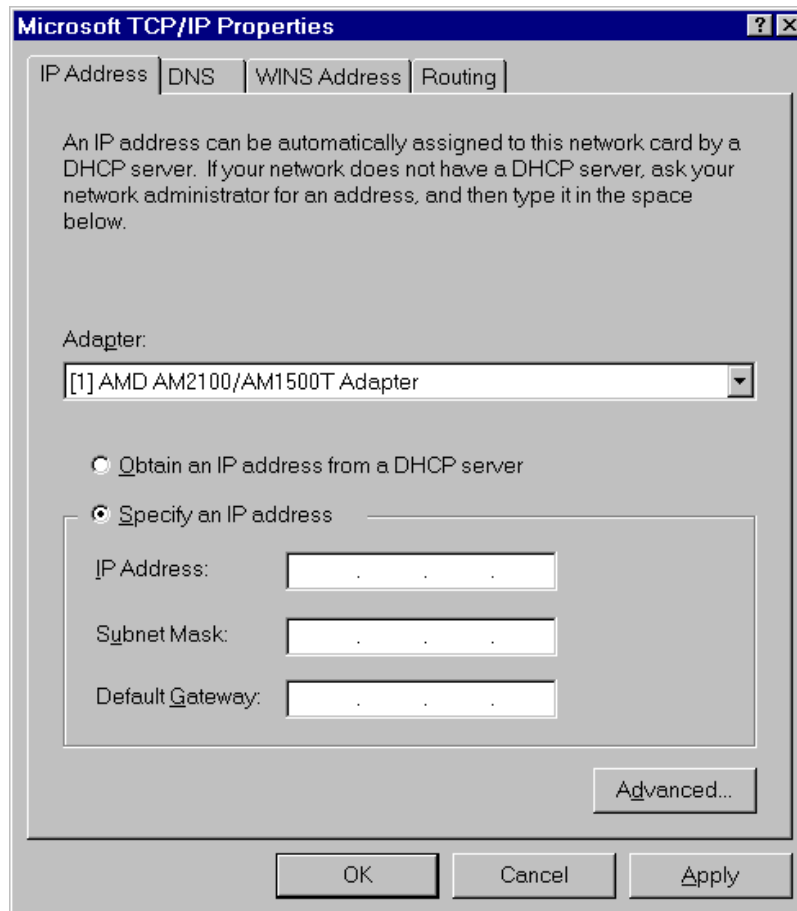
8. Click the **IP Address** tab.

The IP addressing method depends on how your ProxyServer's DHCP Server option was configured. If DHCP Server is active, your IP address is issued automatically. If your network administrator did NOT activate DHCP Services on the ProxyServer, you will have to assign your IP address manually.

Verify the ProxyServer/DHCP status with your network administrator, then proceed to step 9 for DHCP assigned addressing, or to step 10 for manual addressing.

9. If DHCP Services are active on the ProxyServer (the default), verify that the **Obtain an IP address from a DHCP server** option is enabled (checked). At this point, you are done. Go to step 20 and attempt to open an Internet session.

10. If DHCP Services are NOT active on the ProxyServer, you will have to manually enter your IP address. Select manual addressing by clicking the **Specify An IP Address** option. The IP Address and Subnet Mask fields become active.

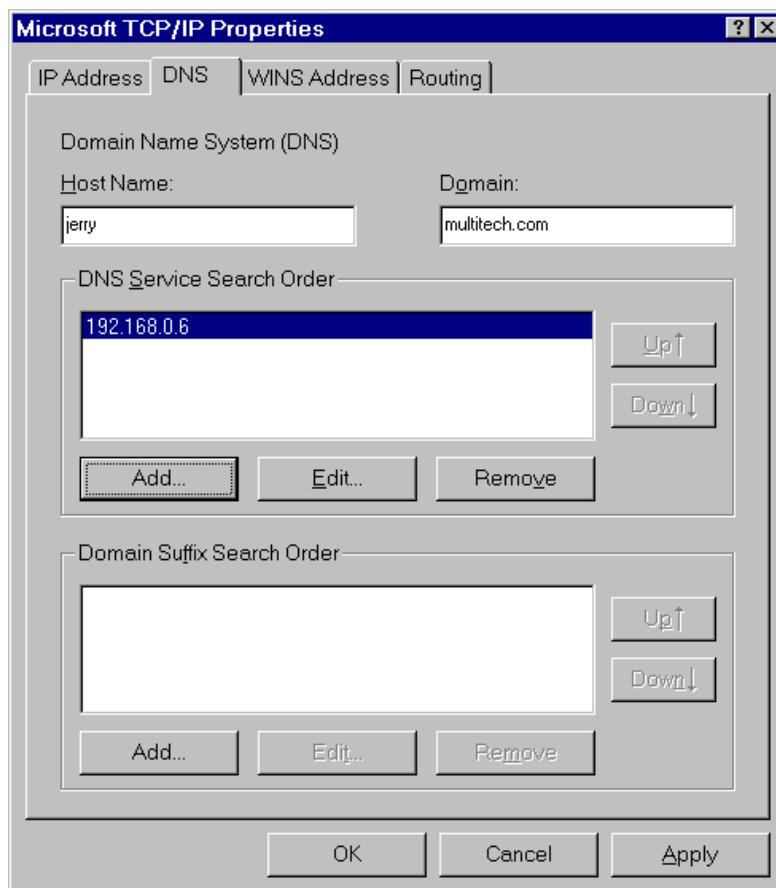


11. In the **IP Address** field, type the IP address assigned to your PC.

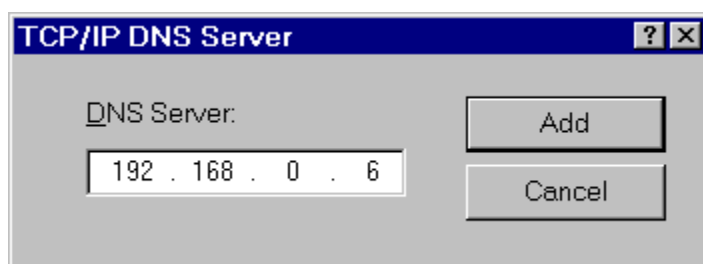
Remove the default IP address (if any), and begin typing the new address. This address is entered in dotted decimal notation and is comprised of four groups (octets) separated by periods or "dots." If a group has fewer than 3 digits, type the necessary digits and press the space bar to move to the next group. When you are finished, verify that the IP address is identical to the IP address you were given for your PC.

12. In the **Subnet Mask** field, type the subnetwork mask assigned by your administrator. When you are finished, verify the new mask.
13. In the Default Gateway field, type the IP address of the gateway assigned to your LAN. When you are finished, verify the new gateway.

14. Click the **DNS** tab. The **Domain Name System (DNS)** properties are displayed.



15. In the **Host Name** field, type your user name (i.e., jerry).
16. In the **Domain** field, enter your company's domain name (usually the company name followed by one of the following extensions: .com, .edu, .gov, .org, .mil, or .net. For example, multitech.com).
17. In the **DNS Server Search Order** group, click **Add**. The **TCP/IP DNS Server** dialog box is displayed.



18. In the **DNS Server** field, place the cursor in the first group and type the IP address of your LAN's DNS server (provided by your network administrator).

19. Click **Add**. You are returned to the **Microsoft TCP/IP Properties** dialog box, **DNS** tab, and the new address is displayed in the **DNS Search Order** list.

Your network may have more than one DNS server, allowing you to use a secondary DNS server if the primary DNS server is not available. If this is the case, add the IP address of the secondary DNS server using the same procedure as with the first.

Note: The address that appears first (at the top of the list) is the primary server (the first one searched). You can use the **Up** and **Down** buttons to rearrange the items in the list, if necessary, until the primary DNS server is listed first.

When this is done, click **OK**. You are returned to the **Network** dialog box.

Use the following checklist to record all the configuration settings for future use:

Configuration Checklist	
IP Address (PC)	. . .
IP Address (ProxyServer)	. . .
Host (User Name)	
Domain	
DNS Server Address	. . .
Network Adapter (Manufacturer/Model Number)	

20. Reboot the PC for changes to take effect.

At this point your client setup is complete. Test your setup by following steps 21 and 22. If you encounter problems, contact you administrator.

21. Initiate an Internet session by double-clicking your browser icon, or try to FTP a file.

Note: The ProxyServer operates transparently, so there should not be a need for any special proxy settings on your IP applications (i.e., browser, Telnet, or FTP). Set up each application as “No Proxy” or equivalent; or, connect to the Internet over the LAN.

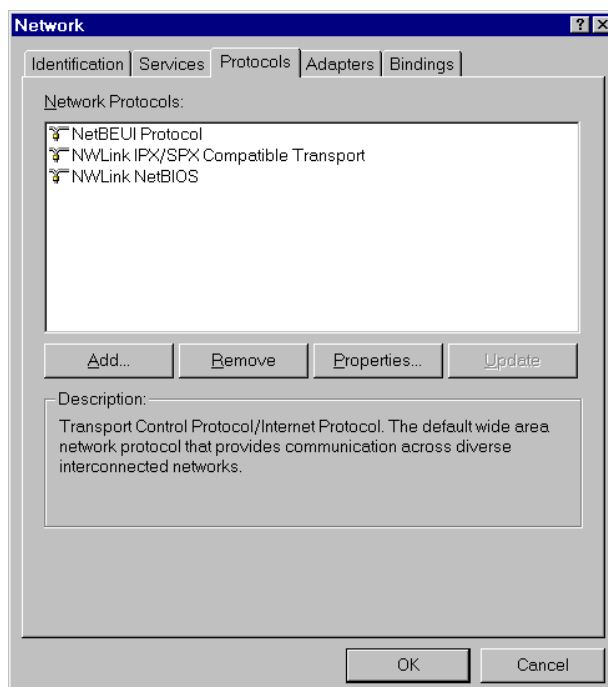
22. To further validate your connection to the ProxyServer, “Ping” the IP address of the ProxyServer.

Installing TCP/IP (WinNT)

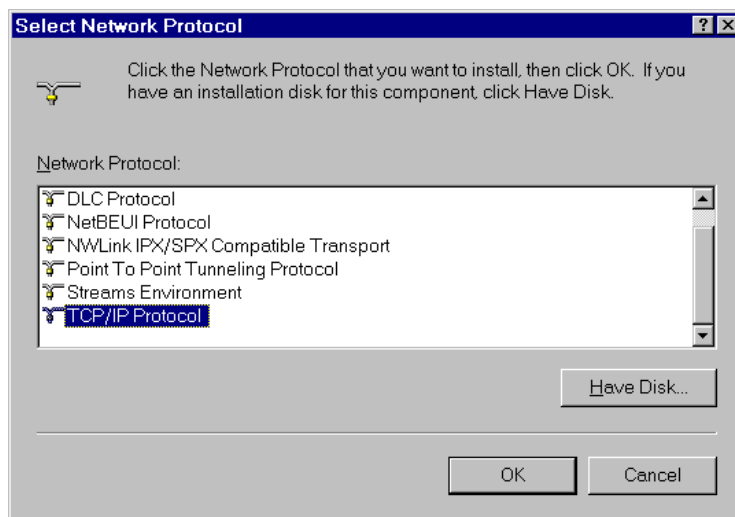
If TCP/IP is not already installed, perform the following steps:

Note: For this procedure you may need your Windows NT installation CD ROM.

1. While the **Network** dialog box is open, click **Add**.



2. The **Select Network Protocol** dialog box is displayed with a list of available protocol options.



Highlight **TCP/IP Protocol** and click **OK**.

If necessary (i.e., the operating system does not find the necessary files on the hard drive), click the **Have Disk** button, then follow the instructions provided on-screen.

3. You are returned to the **Network** dialog.
4. Reboot your PC for changes to take effect.
5. Open the Control Panel and double-click the Network icon to return to the Network Configuration window, then go to step 4 of the **Configuring Windows NT** procedure.



Chapter 6 - RAS Dial-Out Redirector



Introduction

Multi-Tech's Remote Access Server for Microsoft network users enables users to dial-out and fax-out through your MTPSR3-200. Remote Access Solution software uses Multi-Tech's Communications Services Interface (MCSI - pronounced "Mik-see"). MCSI is a software redirector which complies with MCSI/NCSI/NASI defacto standards for software redirection.

The Windows® version of MCSI, called WINMCSI, is supported on Win 3.1x, Windows 98/95, and Windows NT platforms. Since WINMCSI provides data communications connectivity, it needs to be installed and operating before your data communications application software is started.

Installing and Configuring the WINMCSI Modem-Sharing Software

The WINMCSI modem-sharing software (included on the CD) manages access to an Asynchronous Gateway (AG) for outbound calls. It allows Windows communications software packages that do not support INT6B or INT14 to connect to a gateway. It also detects other compatible communications servers (e.g., RASs) on your network and displays the resources they provide to eligible LAN users.

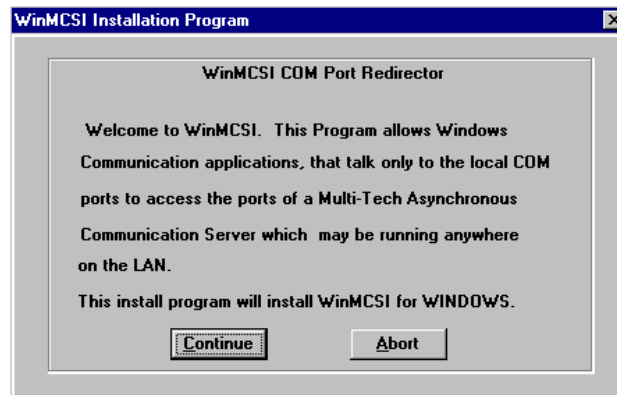
To install WINMCSI in Windows 3.1, Windows for Workgroups 3.11, Windows 98/95, or Windows NT, follow the steps below:

Note: Faxing through WINMCSI is only supported on modems using Lucent chipsets. If you are not certain as to the type of chipset in the internal modem, contact Multi-Tech Systems Technical Support.

1. Power on your client PC and log in to your LAN.
2. Start Windows.
3. Insert the Multi-Tech ProxyServer CD into your CD-ROM drive. The **AutoRun** Install Shield is displayed.
 - Close the **AutoRun** dialog box.
 - Double-click your **My Computer** icon.
 - Right-click the CD-ROM drive icon.
 - Click **Open**. The CD-ROM file displays the following.
 - WINMCSI** - Double-click to open the folder for Windows 3.1 and 3.11 operating systems.
 - W95MCSI** - Double-click to open the folder for Windows 98/95 operating systems.
 - NTMCSI** - Double-click to open the folder for Windows NT operating systems.
4. Begin the software installation:
 - Windows 3.1 and Windows for Workgroups 3.11 users double-click the **Install** icon. Proceed to step 5.
 - Windows 98/95 users double-click the **Inst95** icon. WINMCSI will install as either a 16-bit or 32-bit program, depending on your system. Windows 98/95 will locate the proper install.exe file.
 - If your system is a 16-bit system, proceed to Step 5.
 - If your system is a 32-bit system, proceed to Step 15.
 - Windows NT users double-click the **Setup** icon and proceed to step 15.

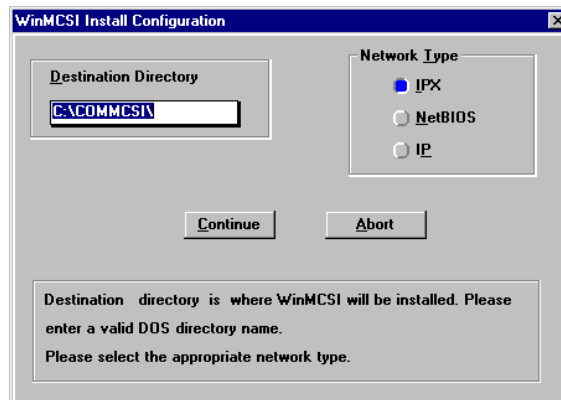
5. If you installed in Windows 3.1, Windows for Workgroups 3.11, or Windows 98/95 (as a 16-bit version):

The **WINMCSI Installation Program** window is displayed.



Click **Continue** to proceed with the installation.

6. The **WinMCSI Install Configuration** window is displayed.

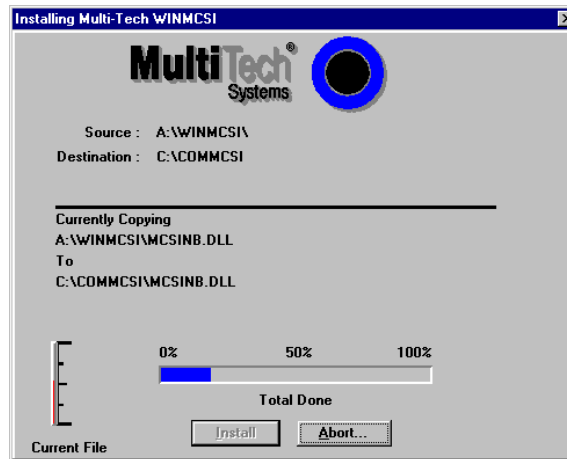


In the **Destination Directory** field, type in the name of the directory to which you want to install WINMCSI, or you can accept the default: C:\COMMCSI.

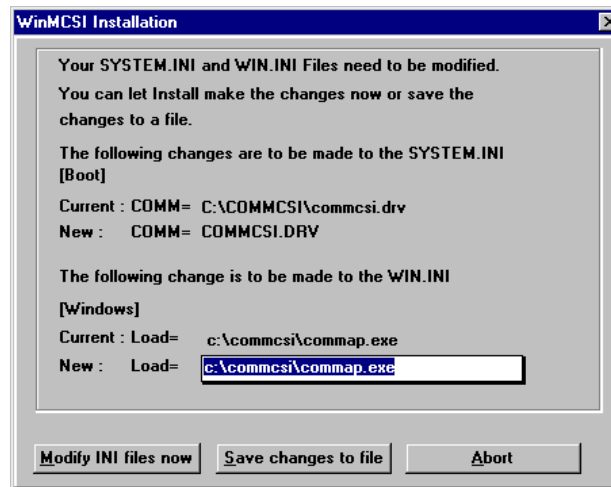
7. In the **Network Type** dialog box, click the appropriate network type (**IP**). Because the default is **IPX**, you will need to select **IP**.

Click **Continue** to proceed with the WINMCSI installation.

8. When the **Installing Multi-Tech WINMCSI** window is displayed, click the Install button to begin the installation. Click **Abort** at any time to cancel the installation



9. When the installation is complete, the **WinMCSI Installation** window is displayed.



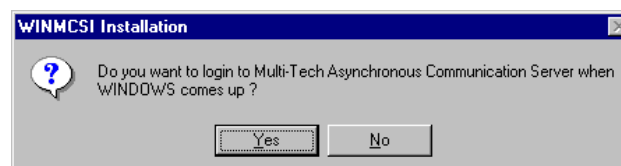
Click **Modify INI files now** to have WINMCSI automatically make changes to your SYSTEM.INI and WIN.INI files.

Click the **Save changes to file** button to have WINMCSI make a copy of the changes to be made and store them in a file.

Note: Because you must make the changes before you can run WINMCSI, it is recommended that you choose **Modify INI files now**.

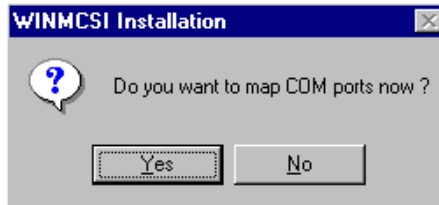
A screen is displayed telling you that your installation is complete and where your WIN.INI and SYSTEM.INI files are backed up.

10. The following message is displayed:



Click **Yes** or **No**, as appropriate.

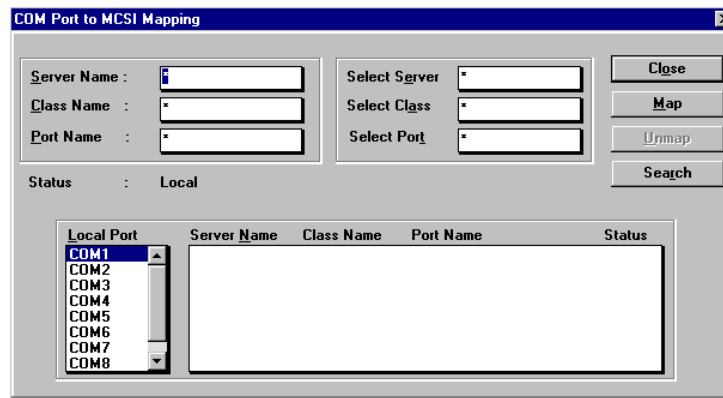
11. The following message is displayed:



If you want to map your COM ports now, click **Yes** and proceed to step 12.

If you want to wait to map your COM Ports until you start WINMCSI, click **No** and proceed to step 13.

12. The **COM Port to MCSI Mapping** window is displayed.



If you want to get the first available line, click **Map** | **Close** and go to the next section.

If you want a specific line, click a COM port in the **Local Port** list box, then click the line to which you want to map that particular COM Port. The status message "Mapped to MCSI" should appear above the Local Port list box.

Click the **Unmap** button if you want to unmap a line.

Click the **Search** button to search for lines on a server.

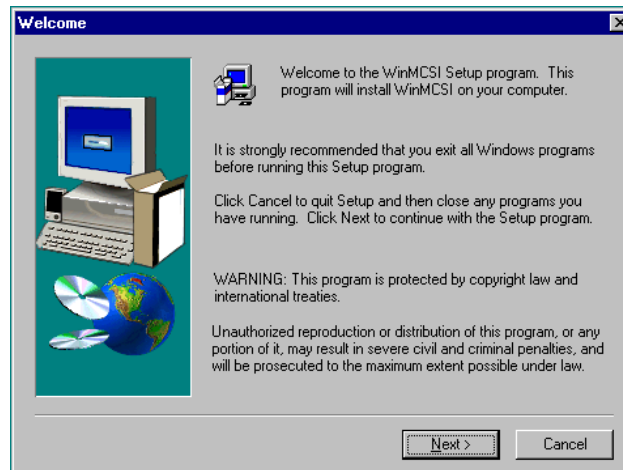
Click the **Close** button when finished.

13. The following message is displayed: "WINMCSI Successfully Installed". Click **OK**.
14. A message is displayed telling you where your old SYSTEM.INI and WIN.INI files have been backed-up. The message also tells you to restart Windows. Click **Restart Windows** to complete the installation.

At this time Your WINMCSI software installation is complete. Proceed to the next section, "Running the WINMCSI Workstation Software."

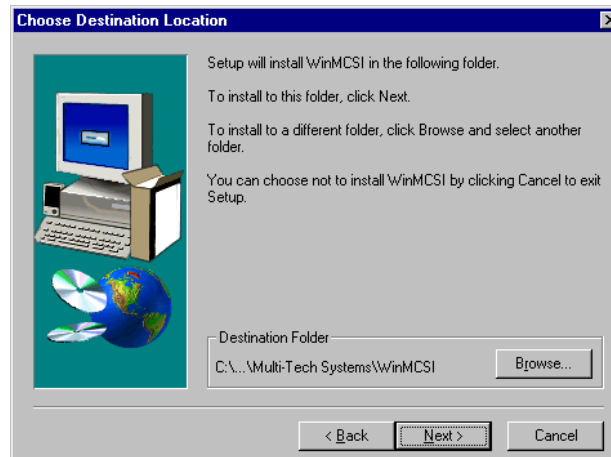
If you installed in Windows 98/95 (as a 32-bit version) or Windows NT:

15. The **Welcome** screen is displayed.



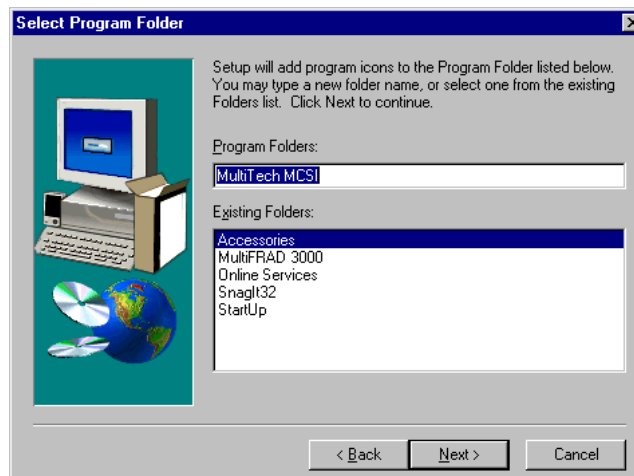
Click **Next** to proceed with the installation.

16. The **Choose Destination Location** screen is displayed.



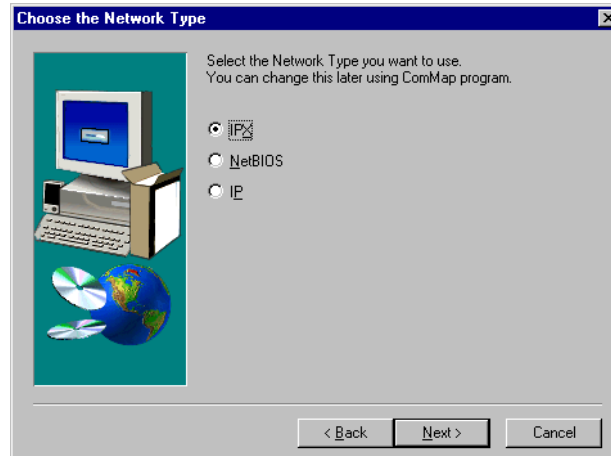
Click **Next** to accept the Destination Folder, or click **Browse** to select a different destination.

17. The **Select Program Folder** screen is displayed.



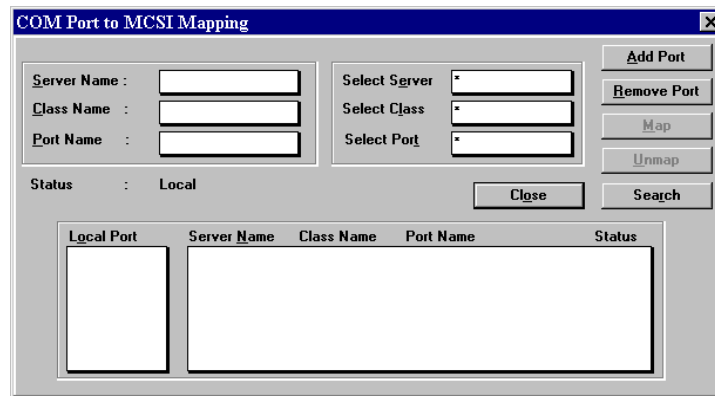
Click **Next** to accept the new folder designation, or choose an existing folder from the list provided.

18. The **Choose Network Type** screen is displayed.



Selections include IPX, NetBIOS, and IP (default is IPX). Click **IP** and then click **Next** to proceed.

19. The **COM Port to MCSI Mapping** window is displayed.



Click **Add Port** to add a port to the **Local Port** list box.

If you want a specific line, click a COM port in the **Local Port** list box, then click the line to which you want to map that particular COM Port. The status message "Mapped to MCSI" should appear above the Local Port list box.

Click **Remove Port** to permanently remove a port from the **Local Port** list box.

Click the **Unmap** button if you want to unmap a line.

Click the **Search** button to search for lines on a server.

Click the **Close** button when finished.

At this time Your WINMCSI software installation is complete. Proceed to the next section, "Running the WINMCSI Workstation Software."

Note: Once MCSI has been installed and configured, make certain that the appropriate modem drivers are installed on the PC you are configuring. Modem drivers can be found in the "Drivers" directory on the ProxyServer CD. Modems using a Rockwell chipset need to install using the 5600.inf file. Modems using a Lucent chipset need to install using the 5634ZDX.inf file. If you are not certain as to the type of chipset in the internal modem, contact Multi-Tech Systems Technical Support.

Running the WINMCSI Workstation Software

WINMCSI has a workstation portion of the software that LAN users run and use to log onto the communications server prior to running datacomm software on their client PCs. The following steps guide you through this process.

1. Start **WINMCSI**.

Windows 3.1, Windows for Workgroups 3.11, or Windows 95 (16-bit) users:

To start WINMCSI, double-click the **ComMap** icon in your Program Manager in Windows. The **ComMap for Windows** window is displayed. Go to step 2.

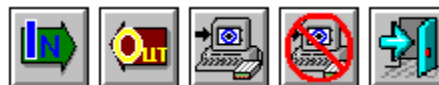
Windows 98/95 (32-bit) and Windows NT users:

To start WINMCSI, click **Start | Programs | MultiTech MCSI | ComMap**.

2. The **ComMap for Windows** window is displayed.



The buttons from left to right are: **Login**, **Logout**, **Map**, **Unmap**, and **Exit**.



3. To setup **ComMap**, click **Setup**.

Click the **Network Type** command. The **Network Type** dialog box is displayed. Your current network type is highlighted. You can change the network type by clicking the option button appropriate for your network. Click **OK** when finished. You must restart Windows if you change this setting.

Note: Do not change the network type unless you have changed the network. Also, make sure that your SYSTEM.INI file contains the device drivers specific to the selected network type.

Click the **Connect Timer** command. The **MCSI Connect Timer** dialog box is displayed. The default value of the connect timer is shown in the Enter Connect Timer Value field. To change the value of the connect timer, type in a different value. Click **OK** when finished.

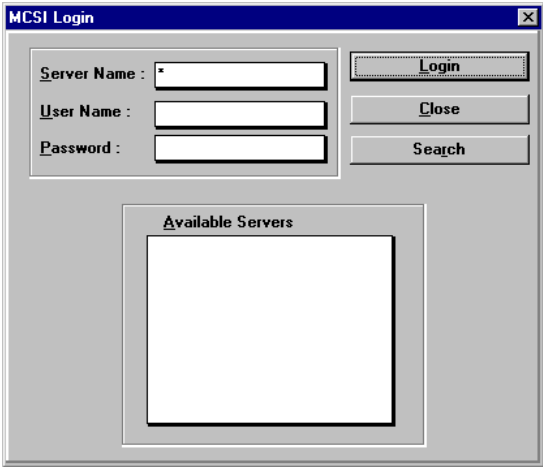
Click the **Baud Change** command. The **ComMap Baud Change** message is displayed. If baud change by an application is permitted, then this command is checked in the Setup Menu. If baud change is unchecked in the Setup Menu, then an application cannot change the baud rate (or other port parameters). Answer the message appropriately.

Click the **Default Login** command. The **Default Login Parameters** dialog box is displayed. Use this dialog box to select a specific RAS to which you want to log into next time Windows is loaded. Click a RAS from the **Available Servers** box. If there are no servers in the Available Servers box, then click the **Search** button. Type in a **User Name** and **Password** (optional) in their respective fields. Click **OK** when finished.

ComMap saves these login parameters in your COMMCSI.INI file.

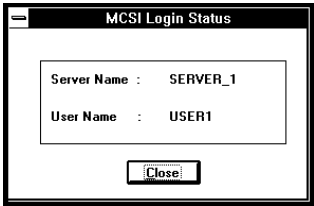
Note: You cannot directly edit the COMMCSI.INI file using a text editor because the password field is encrypted.

- 4. If you have not logged into the network, do so now by clicking **File | Login**, or click the **Login** button. The **MCSI Login** window is displayed.



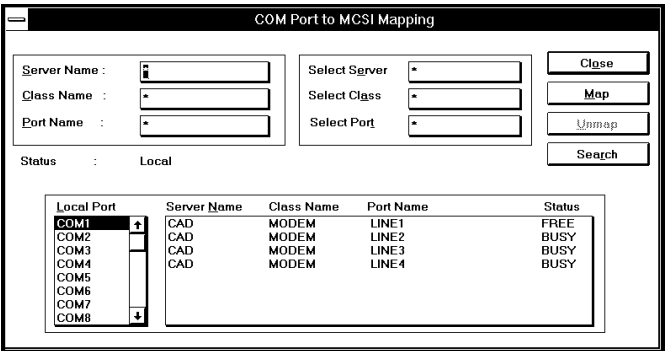
The **Available Servers** box lists the names of the available servers. Click the name of the server to which you want to attach, type a **User Name** and **Password** in their respective fields, and then click **Login**. A window is displayed stating that your login was successful. Click **OK**. If there are no servers listed in the **Available Servers** box, then click the **Search** button to search for a server.

- 5. At the **ComMap for Windows** main window, view your log status by clicking **File | Log Status**. The **MCSI Login Status** window is displayed.



This window shows the name of the server to which you are logged in and the name with which you logged in. Click **Close** when you are finished.

- 6. At the **ComMap for Windows** main window (to map a COM port through MCSI) click **Map | Map**. The **COM Port to MCSI Mapping** window is displayed.



Note: Windows 98/95 users will have two additional buttons in this box, the **Add Port** and the **Remove Port** buttons. You must click the **Add Port** button to view Local Ports. Click the **Remove Port** button to remove Local Ports.

If you want to get the first available line, click the **Map** button and then click the **Close** button and go to step 7.

If you want a specific line, click a COM Port in the Local Port list box, then click the line to which you want to map that particular COM Port. The status message "Mapped to MCSI" should appear above the Local Port list box.

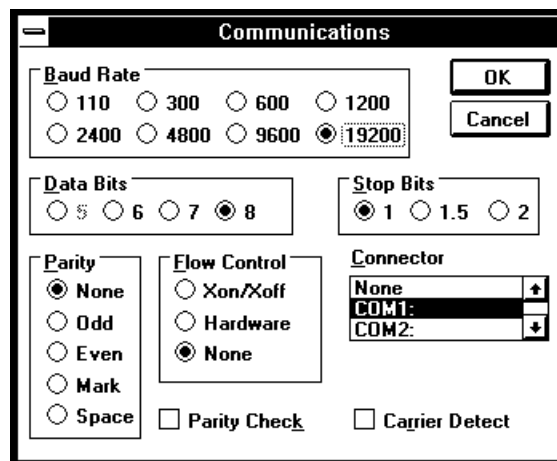
Click **Unmap** if you want to unmap a line.

Click **Search** to search for lines on a server.

Click **Close** when finished.

7. To view a list of mapped COM ports, click **Map | Map List**, or click the **Map** button. Click **Close** when finished.

Below is an example of the Window's Terminal application's (shipped with all versions of Windows) **Communications** dialog box. After mapping your COM Ports with ComMap for Windows, you can check your connectivity and configure your ports with Windows Terminal. It is recommended that you use the settings shown in the example below (in the example COM1 is shown).



8. To unmap a COM port, click **Unmap | Unmap**, or click the **Unmap** button. Click the listing you want to unmap and then click **Unmap**.
9. To logout from the network, click **File | Logout**, or click the **Logout** button.
10. To exit from WINMCSI, click **File | Exit**, or click the **Exit** button. Otherwise you may minimize the screen to minimize WINMCSI to an icon.



Chapter 7 - Remote Configuration



Introduction

This chapter provides procedures for viewing or changing the configuration of a remote unit.

Remote configuration requires the ProxyServer software to be loaded on the local PC. The local PC then controls the remote ProxyServer via the LAN.

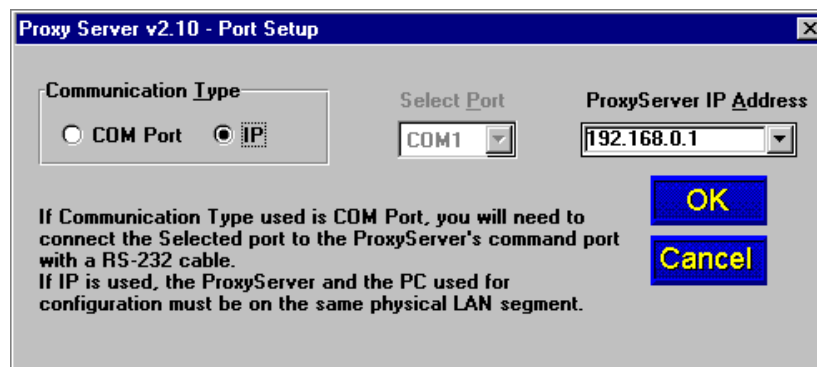
Remote Configuration

Remote configuration is LAN-based and requires a Windows Sockets compliant TCP/IP stack. TCP/IP protocol software that must be installed and functional before the configuration program can be used.

1. You must assign an Internet (IP) address for the PC and for each node that will be managed by the configuration program. Refer to the protocol software documentation for instructions on how to set the IP addresses.

Once you have completed this step, you should be able to use the protocol Ping command for the PC host name. You should also test the network interface configuration by Pinging another TCP/IP device that is connected to the network.

2. Install the ProxyServer software on the local PC. Once installed click **Start | Programs | ProxyServer 2.10 | Configuration Port Setup**.
3. The ProxyServer **Port Setup** dialog box is displayed.

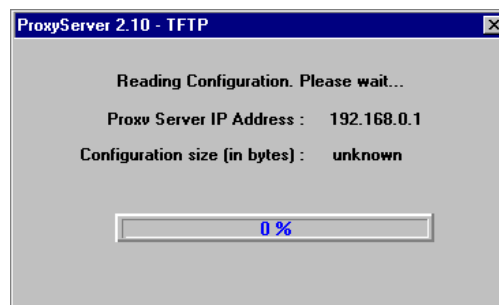


Verify that the **Communication Type** field is set to **IP**.

In the **ProxyServer IP Address** field, enter the IP Address of the remote ProxyServer.

Click **OK** when you are satisfied with your selections.

4. The windows Program Manager menu is displayed.
Double-click the **ProxyServer Configuration** icon.
5. The **Reading Configuration. Please wait ...** screen is displayed.



6. The **Proxy Setup** main menu (for the remote ProxyServer) is then displayed. You can select any of the available buttons and change the configuration (or setup) and download the changes to the remote ProxyServer. Refer to Chapter 4 for a description of the ProxyServer software. For definitions of each dialog box or fields within a dialog box, refer to the on-line **Help** provided in the software.



7. After you have changed the configuration of the remote ProxyServer, click the **Download Setup** button to update the configuration. The remote ProxyServer will be brought down, the new configuration written to the unit, and the unit will reboot.
8. Click the **Exit** button when the downloading is complete.
9. Click the **ProxyServer Configuration** icon in the Program Manager screen to verify that the ProxyServer is running



Chapter 8 - ProxyServer Management



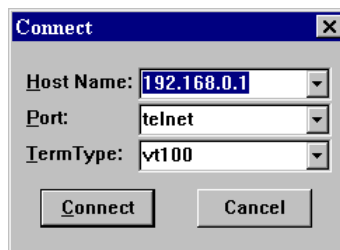
Introduction

A typical Telnet client application and typical Web-browser management of the ProxyServer are described in this chapter. The ProxyServer has a built-in Telnet Server for access through Telnet clients. A typical Telnet client is allowed to configure the ProxyServer and its data ports. In addition, the ProxyServer can be remotely accessed and configured from anywhere on the Internet through its Web interface.

For a detailed description of how the ProxyServer software can work in your environment, refer to Chapter 4 in this User Guide. For a detailed description of each parameter, refer to the on-line Help provided within your ProxyServer software.

The TCP/IP stack has to be loaded before the Telnet client can run and the Telnet Server option in the ProxyServer software has to be enabled. To access the Telnet Client, double click the Telnet icon. A blank Telnet screen is displayed. Click **Connect** and then **Remote System**.

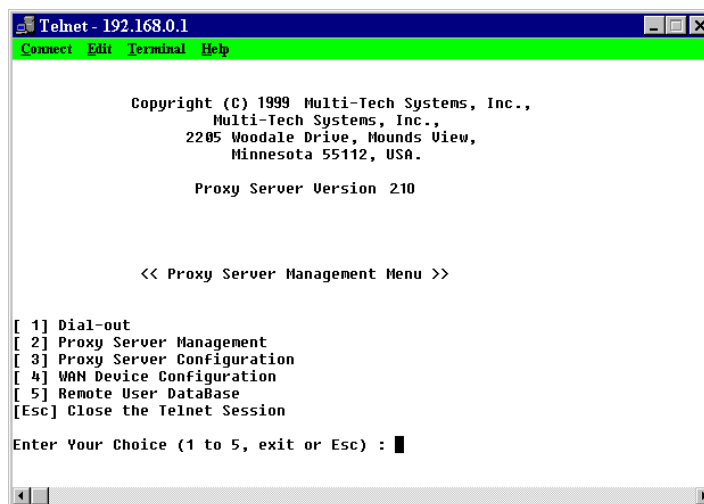
When the **Connect** to remote host dialog box is displayed, a Host Name has to be entered. In this example, the IP Host Name is 192.168.0.1.



Enter your ProxyServer IP Address in the Host Name field. Click the **Connect** button and the ProxyServer Telnet Server dialog box is displayed.

ProxyServer Telnet Server Menu

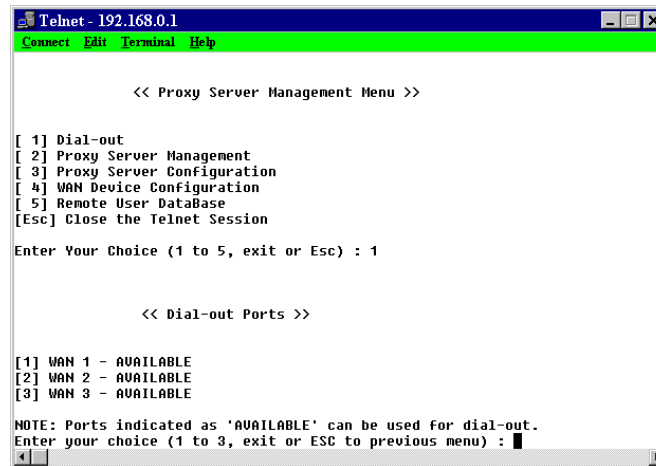
The ProxyServer management menu provides five options; Dial-out, ProxyServer Management, ProxyServer Configuration, WAN Device Configuration, and Remote User Database. The ProxyServer Configuration options allow you to select the protocol stack, high or low level device drivers, applications, filtering, priority, or system information. The Remote User Database option allows you to build and maintain a user database for remote access.



Once you choose an option from the **ProxyServer Telnet Server** dialog box, you must enter your password before your choice is accepted. The password must be the same as the server password entered in the **Applications Setup** dialog box in the ProxyServer software.

Dial-Out

The dial-out option (Option 1) enables a Telnet user to configure one of the WAN ports for a dial-out session. The default configuration of 115200 bps, 8N1 can be used for the dial-out session, or the user can specify each parameter for the port (e.g., the baud rate, number of data bits, parity, or number of stop bits). When the connection is established, anything entered on the keyboard is immediately presented to the WAN port. When the dial-out session is over, the WAN port reverts to its original configuration.



```

Telnet - 192.168.0.1
Connect Edit Terminal Help

<< Proxy Server Management Menu >>

[ 1] Dial-out
[ 2] Proxy Server Management
[ 3] Proxy Server Configuration
[ 4] WAN Device Configuration
[ 5] Remote User DataBase
[Esc] Close the Telnet Session

Enter Your Choice (1 to 5, exit or Esc) : 1

<< Dial-out Ports >>

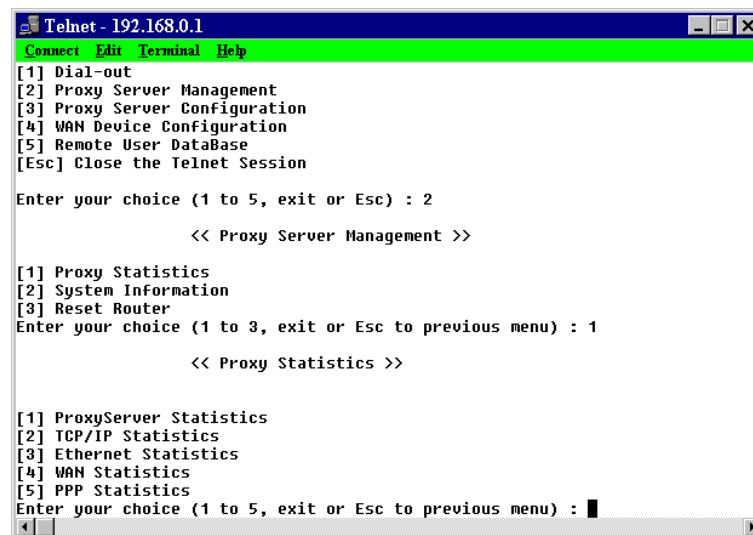
[1] WAN 1 - AVAILABLE
[2] WAN 2 - AVAILABLE
[3] WAN 3 - AVAILABLE

NOTE: Ports indicated as 'AVAILABLE' can be used for dial-out.
Enter your choice (1 to 3, exit or ESC to previous menu) :

```

ProxyServer Management

The ProxyServer Management option (Option 2) provides three options; statistics, system information, or to reset the ProxyServer. The statistics option allows you to view stats on the ProxyServer, Ethernet port, WAN port, etc. The system information allows you to view stats on the firmware version, memory size, etc.



```

Telnet - 192.168.0.1
Connect Edit Terminal Help

[1] Dial-out
[2] Proxy Server Management
[3] Proxy Server Configuration
[4] WAN Device Configuration
[5] Remote User DataBase
[Esc] Close the Telnet Session

Enter your choice (1 to 5, exit or Esc) : 2

<< Proxy Server Management >>

[1] Proxy Statistics
[2] System Information
[3] Reset Router
Enter your choice (1 to 3, exit or Esc to previous menu) : 1

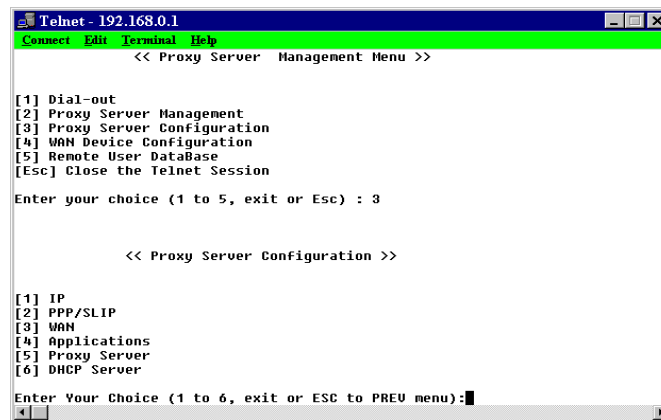
<< Proxy Statistics >>

[1] ProxyServer Statistics
[2] TCP/IP Statistics
[3] Ethernet Statistics
[4] WAN Statistics
[5] PPP Statistics
Enter your choice (1 to 5, exit or Esc to previous menu) :

```

ProxyServer Configuration

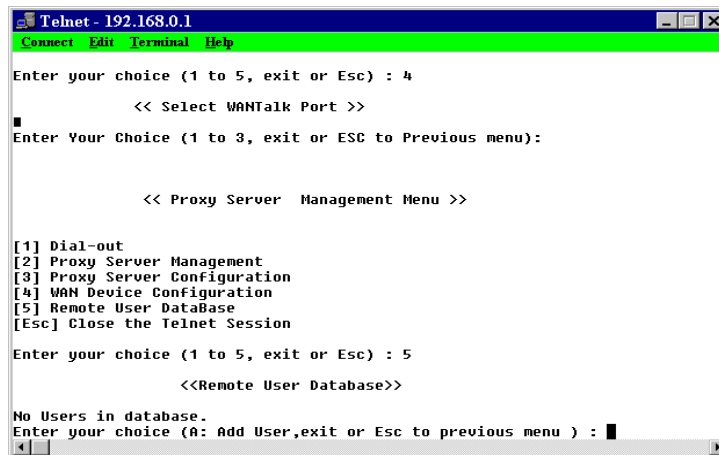
The ProxyServer Configuration option allows you to view and change parameters on the protocol stacks, high and low level device drivers, enable or disable the supported servers, configure Mux data ports, set up filtering and priority, or view system information.



To select an option, enter the number of the option and hit the Enter key. For example, to select the Protocol Stacks option, type **1** <Enter>. For details on a parameter, refer to the on-line helps.

Remote User Database

The Remote User Database option from the ProxyServer management menu allows you to add and configure a list of users who will access the ProxyServer remotely. After selecting Remote User Database (type **2** <Enter>) from the main menu, type **A** <Enter> to add a new user to the database. The following list of options is displayed:



By selecting and configuring the various options and entering the desired information, you can construct a database of remote users for the ProxyServer. For a detailed description of each option, refer to the on-line Help provided in your ProxyServer software.

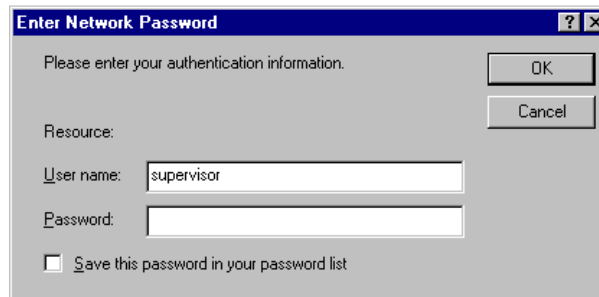
Web Browser Management

The ProxyServer can be accessed from anywhere on the connected Internet via the built-in Web Browser interface. You must check this option in Other setup to enable the function. Depending on the rights of the user (read/write, or read only), it is possible to view the current parameters and statistics of the ProxyServer as well as configure and download setup changes to the ProxyServer.

You can access ProxyServer configuration by typing the **IP Address** of the unit into the address line of your web browser. In this example, the IP address is 192.168.0.1.

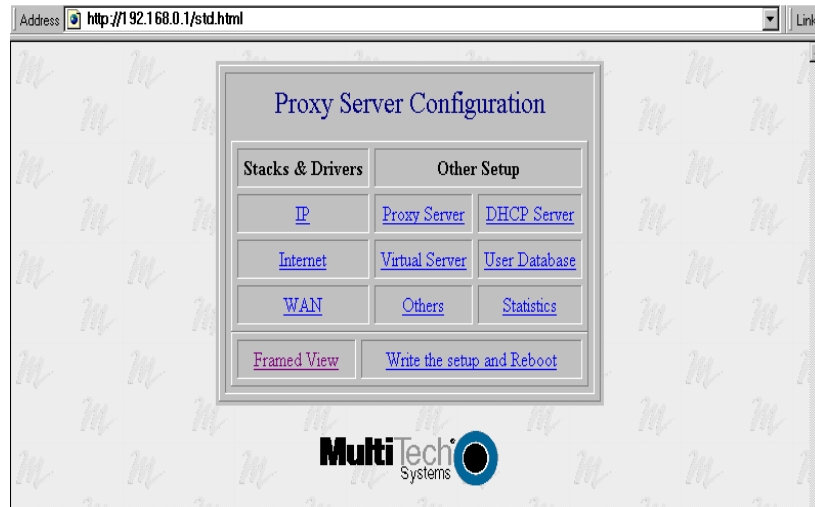


Click the word **Login** to gain access to the ProxyServer. The following screen is displayed:



Enter the proper **User Name** and **Password**, and then click **OK**.

The ProxyServer Configuration menu page is displayed.



Note: The first user to access the ProxyServer will have *read/write* rights over the unit. All subsequent users will have *read only* rights, and therefore, some of the options within the Web interface will be inactive (i.e., will not be linked).

From the ProxyServer Configuration menu, you can access current settings and view statistics, as well as configure and download a new setup to the ProxyServer.



Chapter 9 - Service, Warranty and Tech Support



Introduction

This chapter will provide you the resources for receiving service or support for your ProxyServer. The chapter starts with a description of the warranty, and continues with instructions for contacting the Service department, Technical Support group, and various Multi-Tech Internet resources.

Limited Warranty

Multi-Tech Systems, Inc. ("MTS") warrants that its products will be free from defects in material or workmanship for a period of two years from the date of purchase, or if proof of purchase is not provided, two years from date of shipment. MTS MAKES NO OTHER WARRANTY, EXPRESSED OR IMPLIED, AND ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE HEREBY DISCLAIMED. This warranty does not apply to any products which have been damaged by lightning storms, water, or power surges or which have been neglected, altered, abused, used for a purpose other than the one for which they were manufactured, repaired by the customer or any party without MTS's written authorization, or used in any manner inconsistent with MTS's instructions.

MTS's entire obligation under this warranty shall be limited (at MTS's option) to repair or replacement of any products which prove to be defective within the warranty period, or, at MTS's option, issuance of a refund of the purchase price. Defective products must be returned by Customer to MTS's factory transportation prepaid.

MTS WILL NOT BE LIABLE FOR CONSEQUENTIAL DAMAGES AND UNDER NO CIRCUMSTANCES WILL ITS LIABILITY EXCEED THE PURCHASE PRICE FOR DEFECTIVE PRODUCTS.

On-line Warranty Registration

If you would like to register your ProxyServer electronically, you can do so at the following address:

<http://www.multitech.com/register/>

Tech Support

Multi-Tech has an excellent staff of technical support personnel available to help you get the most out of your Multi-Tech product. If you have any questions about the operation of this unit, call 1-800-972-2439. Please fill out the ProxyServer information (below), and have it available when you call. If your ProxyServer requires service, the tech support specialist will guide you on how to send in your equipment (refer to the next section).

Recording ProxyServer Information

Please fill in the following information on your ProxyServer. This will help tech support in answering your questions. (The same information is requested on the Warranty Registration Card.)

Model No.: _____
Serial No.: _____
Software Version: _____

The model and serial numbers are on the bottom of your ProxyServer.

Please note the status of your ProxyServer beofre calling tech support. You should include LED indicators, screen messages, diagnostic test results, problems with a specific application, etc. Use the space below to note the status:

Contacting Tech Support via E-mail

If you prefer to receive service on-line, via the Internet, you can contact Tech Support via e-mail at the following address:

http://www.multitech.com/_forms/email_tech_support.htm

Service

If your tech support specialist decides that service is required, your ProxyServer can be sent (freight prepaid) to our factory. Return shipping charges will be paid by Multi-Tech Systems.

Include the following with your ProxyServer:

- a description of the problem.
- return billing and return shipping addresses.
- contact name and phone number.
- check or purchase order number for payment if the ProxyServer is out of warranty. (Check with your technical support specialist for the standard repair charge for your ProxyServer).
- if possible, note the name of the technical support specialist with whom you spoke.

If you need to inquire about the status of the returned product, be prepared to provide the **serial number** of the product sent.

Send your ProxyServer to this address:

MULTI-TECH SYSTEMS, INC.
2205 WOODALE DRIVE
MOUNDS VIEW, MINNESOTA 55112
ATTN: SERVICE OR REPAIRS

You should also check with the supplier of your ProxyServer on the availability of local service and/or loaner units in your area.

The Multi-Tech BBS

For customers who do not have Internet access, Multi-Tech maintains a bulletin board system (BBS) that mirrors its FTP site. Information available from the BBS includes new product information, product upgrade files, and problem-solving tips. The phone number for the Multi-Tech BBS is (800) 392-2432 (USA and Canada) or (612) 785-3702 (international and local).

The BBS can be accessed by any asynchronous modem operating at 1200 bps to 33,600 bps at a setting of 8 bits, no parity, and 1 stop bit (8-N-1).

To log on to the Multi-Tech BBS

1. Set your communications program to **8-N-1**.
2. Dial our BBS at (800) 392-2432 (USA and Canada) or (612) 785-3702 (international and local).
3. At the prompts, type your first name, last name, and password; then press ENTER. If you are a first time caller, the BBS asks if your name is spelled correctly. If you answer yes, a questionnaire is displayed. You must complete the questionnaire to use the BBS on your first call.
4. Press ENTER until the Main Menu is displayed. From the Main Menu you have access to two areas: the Files Menu and News. For help on menu commands, type **?**.

To Download a file

If you know the file name

1. From the Main Menu, type **F** to access the Files Menu, then type **D**.
2. Enter the name of the file you wish to download from the BBS.
3. If a password is required, enter the password.
4. Answer **Y** or **N** to the automatic logoff question.
5. Select a file transfer protocol by typing the indicated letter, such as **Z** for Zmodem (the recommended protocol).
6. If you select Zmodem, the transfer will begin automatically. If you select another protocol, you may have to initiate the transfer yourself. (In most datacomm programs, the PAGE DOWN key initiates the download.)
7. When the download is complete, press ENTER to return to the File Menu.
8. To exit the BBS, type **G** and press ENTER.

If you don't know the file name

1. From the Main Menu, type **F** to access the Files Menu. For a list of file areas, type **L**, press ENTER, then type **L** and press ENTER again. (If you do not type the second **L**, you will list all of the files on the BBS.)
2. Mark each file area you would like to examine by typing its list number and pressing ENTER.
3. Enter **L** to list all the files in the selected file areas. Enter **C** to go forward in the file list and **P** to go back.
4. To mark one or more files for download, type **M**, press ENTER, type the list numbers of the files, and press ENTER again.
5. Enter **D**. You will see a list of the files you have marked. Enter **E** if you would like to edit the list; otherwise enter **D** again to start the download process.

6. Select a file transfer protocol by typing the indicated letter, such as **Z** for Zmodem (the recommended protocol).
7. If you select Zmodem, the file will transfer automatically. If you select another protocol, you may have to initiate the transfer yourself. (In most data communications programs, the PAGE DOWN key initiates the download.)
8. When the download is complete, press ENTER to return to the File Menu.
9. To exit the BBS, type **G** and press ENTER.

About the Internet

Multi-Tech is a commercial user on the Internet, and we retrieve messages from our customers on a periodic basis. Multi-Tech's presence includes a Web site at:

<http://www.multitech.com>

and an FTP site at:

<ftp://ftp.multitech.com>

Ordering Accessories

SupplyNet, Inc. supplies replacement transformers, cables and connectors for select Multi-Tech products. You can place an order with SupplyNet via mail, phone, fax or the Internet at:

Mail: SupplyNet, Inc.
614 Corporate Way
Valley Cottage, NY 10989

Phone: 800 826-0279

Fax: 914 267-2420

Email: info@thesupplynet.com

Internet: <http://www.thesupplynet.com>

SupplyNet On-line Ordering Instructions

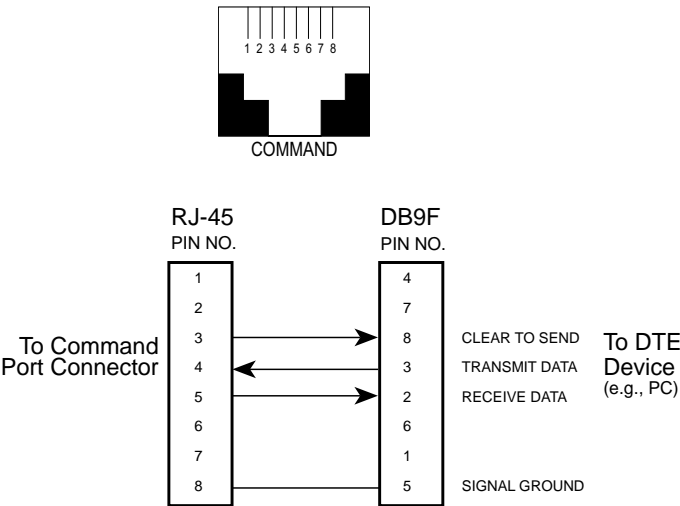
1. Browse to <http://www.thesupplynet.com>. In the **Browse by Manufacturer** drop-down list, select **Multi-Tech** and click 
2. To order, type in quantity, and click 
3. Click  to change your order
4. After you have selected all of your items click  to finalize the order. The SupplyNet site uses Verisign's Secure Socket Layer (SSL) technology to ensure your complete shopping security.

Proxy*Server* 200-Series

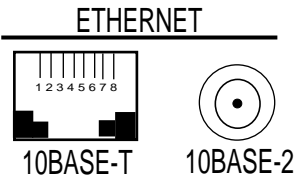
Appendices

Appendix A - Cabling Diagrams

Command Port Cable

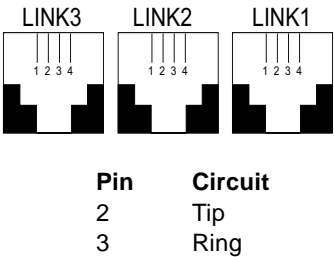


LAN Cables

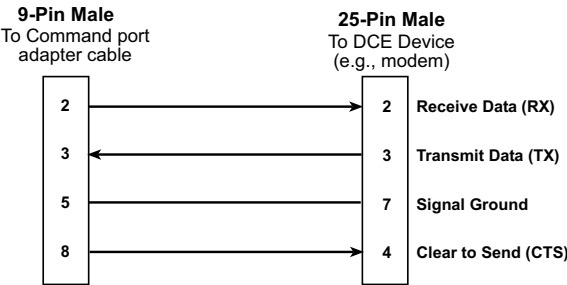


Pin	Circuit Signal Name	Pin	Description
1	TD+ Data Transmit Positive	1	Center
2	TD- Data Transmit Negative	2	Shield
3	RD+ Data Receive Positive		
6	RD- Data Receive Negative		

WAN Cables



Remote Configuration Cable



Appendix B - Script Commands

A script file can be used to automate certain operations. The script file is a text file containing a sequence of the following commands (listed here according to their functions). This is similar to what you will find in the Help file in your ProxyServer software. Following the list of commands is an example script.

Commands (by Function)

Dial, Connection and Remote

ACTIVATEDOD	BAUDRATE	BREAK
GETCTS	GETDCD	HANGUP
PARITYR	GETC	RGETS
RXFLUSH	SETDTR	SETRTS
STOPBITS	THISLAYERUP	TRANSMIT
TXFLUSH	WAITFOR	

Mathematical functions

DEC	INC
-----	-----

Miscellaneous

EXIT	WAIT
------	------

Program constructs

FOR	IF	PROC
SWITCH	WHILE	

String operations

ATOI	ITOA	STRCAT
STRCMP	STRCOPY	STRFMT
STRLEN	TOLOWER	TOUPPER

Example Script:

```
proc main;
    string login_prompt;
    string user_name;
    string password_prompt;
    string password;
    string shell_menu;
    string shell_menu_response;
    integer timeout;

    timeout=10;
    login_prompt="login:";
    user_name="user1";
    password_prompt="Password:";
    password="user1";
    shell_menu="choice:";
    shell_menu_response="1";

    transmit("A");
    wait(1)
    transmit("T^M");
    waitfor ("OK",10);

    transmit ("A");
    wait (1);
    transmit ("T");
    wait (1);
    transmit ("DT963^M");

    if (waitfor (login_prompt,60)) then
        transmit (user_name);
        transmit ("^M");
        if (waitfor (password_prompt,timeout)) then
            transmit (password);
            transmit ("^M");
            if (waitfor (shell_menu,timeout)) then
                transmit (shell_menu_response);
                transmit ("^M");
            else
                transmit ("Shell Menu Not Received^M");
            endif
        else
            transmit ("Password Prompt Not Received^M");
        endif
    else
        transmit ("Login Prompt Not Received^M");
    endif
endproc
```

Appendix C - Regulatory Information

Class B Statement

FCC Part 15

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC rules.

Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference.
- (2) This device must accept any interference that may cause undesired operation.

Warning: Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Industry Canada

This Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

FCC Regulations for Telephone Line Interconnection

1. This equipment complies with Part 68 of the Federal Communications Commission (FCC) rules. On the outside surface of this equipment is a label that contains, among other information, the FCC registration number and ringer equivalence number (REN). If requested, this information must be provided to the telephone company.
2. As indicated below, the suitable jack (Universal Service Order Code connecting arrangement) for this equipment is shown. If applicable, the facility interface codes (FIC) and service order codes (SOC) are shown. An FCC-compliant telephone cord and modular plug is provided with this equipment. This equipment is designed to be connected to the telephone network or premises wiring using a compatible modular jack which is Part 68 compliant. See installation instructions for details.
3. The ringer equivalence number (REN) is used to determine the number of devices which may be connected to the telephone line. Excessive REN's on the telephone line may result in the devices not ringing in response to an incoming call. In most, but not all areas, the sum of the REN's should not exceed five (5.0). To be certain of the number of devices that may be connected to the line, as determined by the total REN's, contact the telephone company to determine the maximum REN for the calling area.
4. If this equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice isn't practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.
5. The telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make necessary modifications in order to maintain uninterrupted service.
6. If trouble is experienced with this equipment (the model of which is indicated below) please contact Multi-Tech Systems, Inc., at the address shown below for details of how to have repairs made. If the equipment is causing harm to the telephone network, the telephone company may request that you remove the equipment from the network until the problem is resolved.
7. No repairs are to be made by you. Repairs are to be made only by Multi-Tech Systems or its licensees. Unauthorized repairs void registration and warranty.
8. This equipment cannot be used on public coin service provided by the telephone company. Connection to Party Line Service is subject to state tariffs. (Contact the state public utility commission, public service commission or corporation commission for information.)
9. If so required, this equipment is hearing-aid compatible.

Manufacturer:	Multi-Tech Systems, Inc.
Trade name:	ProxyServer 200-Series
Model Numbers:	MTPSR3-200
FCC Registration Number:	AU7USA-24994-M5-E
Ringer Equivalence:	0.6B
Modular Jack (USOC):	RJ-11
Service Center in U.S.A.:	Multi-Tech Systems Inc. 2205 Woodale Drive Mounds View, MN 55112 (800) 328-9717 (612) 785-3500 (612) 785-9874 FAX

Canadian Limitations Notice:

RINGER EQUIVALENCE NUMBER

NOTICE: The ringer equivalence number (REN) assigned to each terminal device provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the ringer equivalence numbers of all the devices does not exceed 5.

NOTICE: The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operational and safety requirements. The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations. Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

EMC and Safety Directive Compliance



The CE mark is affixed to this Multi-Tech product to confirm compliance with the following European Community Directives:

Council Directive 89/336/EEC of 3 May 1989 on the approximation of the laws of Member States relating to electromagnetic compatibility.

and

Council Directive 73/23/EEC of 19 February 1973 on the harmonization of the laws of Member States relating to electrical equipment designed for use within certain voltage limits:

each amended by

Council Directive 93/68/EEC of 22 July 1993 on the harmonization of CE marking requirements.

Appendix D - AT Command Summary

This section summarizes your modem's AT commands. For detailed information on the commands, download ZPXHELP.EXE from the Multi-Tech BBS (see "Multi-Tech BBS" in Chapter 9).

AT Commands

Command: **+++AT<CR>** **Escape Sequence**

Values: n/a

Description: Puts the modem in command mode (and optionally issues a command) while remaining on-line. Type **+++AT** and up to ten command characters, then press ENTER. Used mostly to issue the hang-up command: **+++ATH<CR>**.

Command: **AT** **Attention Code**

Values: n/a

Description: The attention code precedes all command lines except **A/** and the escape sequence.

Command: **ENTER Key**

Values: n/a

Description: Press the ENTER key to execute most commands.

Command: **\$** **Detect AT&T's "call card" tone**

Values: n/a

Description: This symbol placed in dialing string enables the modem to detect AT&T's "call card" tones to access user's calling card when originating an on-line connection--

ATDT¹⁰²⁸⁸⁰⁶¹²⁷⁸⁵³⁵⁰⁰**\$**¹²³⁴⁵⁶⁷⁸⁹
(access/phone number) (Credit Card number)

Command: **A** **Answer**

Values: n/a

Description: Answer an incoming call before the final ring.

Command: **A/** **Repeat Last Command**

Values: n/a

Description: Repeat the last command string. Do not precede this command with **AT**. Do not press ENTER to execute.

Command: **Bn** **Communication Standard Setting**

Values: $n = 0-3, 15, 16$

Default: 1 and 16

Description: B0 Select ITU-T V.22 mode when modem is at 1200 bps.
 B1 Select Bell 212A when modem is at 1200 bps.
 B2 Deselect V.23 reverse channel (same as B3).
 B3 Deselect V.23 reverse channel (same as B2).
 B15 Select V.21 when the modem is at 300 bps.
 B16 Select Bell 103J when the modem is at 300 bps.

Command: **Cn** **Carrier Control**

Values: $n = 1$

Default: 1

Description: C0 Transmit carrier always off. (Not supported.)
 C1 Normal transmit carrier switching (included for backward compatibility with some software).

Command: **Ds** **Dial**

Values: $s =$ dial string (phone number and dial modifiers)

Default: none

Description: Dial telephone number s , where s may up to 40 characters long and include the 0-9, *, #, A, B, C, and D characters, and the **L**, **P**, **T**, **V**, **W**, **S**, comma (,), semicolon (;), !, @, ^ and \$ dial string modifiers.

Dial string modifiers:

- L** Redial last number. (Must be placed immediately after **ATD**.)
- P** Pulse-dial following numbers in command .
- T** Tone-dial following numbers in command (default).
- V** Switch to speakerphone mode and dial the following number. Use **ATH** command to hang up.
- W** Wait for a new dial tone before continuing to dial. (**X2**, **X4**, **X5**, **X6**, or **X7** must be selected.)
- S** Dial a telephone number previously stored using the **&Zn=x** command (see **&Zn=x** command for further information). The range of *n* is 0-3.
- ,** Pause during dialing for time set in register **S8**.
- ;** Return to command mode after dialing. (Place at end of dial string.)
- !** Hook flash. Causes the modem to go on-hook for one-half second, then off-hook again.
- @** Wait for quiet answer. Causes modem to wait for a ringback, then 5 seconds of silence, before processing next part of command. If silence is not detected, the modem returns a NO ANSWER code.
- \$** AT&T's "call card" tones detection.
- ^** Disable data calling tone transmission.

Command: **DS=n** **Dial Stored Telephone Number**

Values: *n* = 0–3

Default: none

Description: Dial a number previously stored in directory number *n* by the **&Zn=x** command .
Example: **ATDS=3**

Command: **En** **Echo Command Mode Characters**

Values: *n* = 0 or 1

Default: 1

Description: E0 Do not echo keyboard input to the terminal.
E1 Do echo keyboard input to the terminal.

Command: **Fn** **Echo On-line Data Characters**

Values: *n* = 1

Default: 1

Description: F0 Enable on-line data character echo. (Not supported.)
F1 Disable on-line data character echo (included for backward compatibility with some software).

Command: **Hn** **Hook Control**

Values: *n* = 0 or 1

Default: 0

Description: H0 Go on-hook to hang up.
H1 Go off-hook to make the phone line busy.

Command: **In** **Information Request**

Values: *n* = 0–4, 9, 11

Default: None

Description: I0 Display default speed and controller firmware version.
I1 Calculate and display ROM checksum (e.g., "12AB").
I2 Check ROM and verify the checksum, displaying **OK** or **ERROR**.
I3 Display default speed and controller firmware version.
I4 Display firmware version for data pump (e.g., "94").
I9 Display country code (e.g., "NA Ver. 1").
I11 Display Diagnostic Information for the last Modem Connection (i.e., DSP and Firmware version, Link Type, Line Speed, Serial Speed, Type of Error Correction/Data Compression, Number of past Retrans, etc.)

Command: **Ln** **Monitor Speaker Volume**

Values: *n* = 0, 1, 2, or 3

Default: 2

Description: L0 Select low volume.
L1 Select low volume.
L2 Select medium volume.
L3 Select high volume.

Command: Mn Monitor Speaker Mode

Values: $n = 0, 1, 2, \text{ or } 3$

Default: 1

Description: M0 Speaker always off.
M1 Speaker on until carrier signal detected.
M2 Speaker always on when modem is off-hook.
M3 Speaker on until carrier is detected, except while dialing.

Command: Nn Modulation Handshake

Values: $n = 0 \text{ or } 1$

Default: 1

Description: N0 Modem performs handshake only at communication standard specified by S37 and the **B** command.
N1 Modem begins handshake at communication standard specified by S37 and the **B** command. During handshake, fallback to a lower speed can occur.

Command: O Return On-line to Data Mode

Values: 0, 1, 3

Default: None

Description: O0 Exit on-line command mode and return to data mode.
O1 Issue a retrain and return to on-line data mode.
O3 Issue a rate renegotiation and return to data mode.

Command: Qn Result Codes Enable/Disable

Values: $n = 0 \text{ or } 1$

Default: 0

Description: Q0 Enable result codes.
Q1 Disable result codes.

Command: Sr=n Set Register Value

Values: $r = \text{S-register number}; n \text{ varies}$

Default: None

Description: Set value of register Sr to value of n , where n is entered in decimal format.

Command: Sr? Read Register Value

Values: $r = \text{S-register number}$

Default: None

Description: Read value of register Sr and display value in 3-digit decimal form.

Command: Vn Result Code Format

Values: $n = 0 \text{ or } 1$

Default: 1

Description: V0 Displays result codes as digits (terse response).
V1 Displays result codes as words (verbose response).

Command: Xn Result Code Selection

Values: $n = 0-7$

Default: 4

Description: X0 Basic result codes (e.g., *CONNECT*); does not look for dial tone or busy signal.
X1 Extended result codes (*CONNECT 56000 V42bis*, *CONNECT 33600 V42bis*, etc.); does not look for dial tone or busy signal.
X2 Extended result codes with *NO DIALTONE*; does not look for busy signal.
X3 Extended result codes with *BUSY*; does not look for dial tone.
X4 Extended result codes with *NO DIALTONE* and *BUSY*.
X5 Extended result codes with *NO DIALTONE* and *BUSY*.
X6 Extended result codes with *NO DIALTONE* and *BUSY*.
X7 Basic result codes with *NO DIALTONE* and *BUSY*.

Command:	Yn	Long Space Disconnect
Values:		$n = 0$
Default:		0
Description:	Y0	Disable sending or responding to long space break signal on disconnect.
	Y1	Enable sending or responding to long space break signal on disconnect. (Not supported.)
Command:	Zn	Modem Reset
Values:		$n = 0$ or 1
Default:		None
Description:	Z0	Reset modem to profile saved by the last &W command.
	Z1	Same as Z0.
Command:	&Bn	V.32 Auto Retrain
Values:		$n = 1$
Default:		1
Description:	&B0	Disable V.32 auto retrain. (Not supported.)
	&B1	Enable V.32 auto retrain.
Command:	&Cn	Data Carrier Detect (DCD) Control
Values:		$n = 0$ or 1
Default:		1
Description:	&C0	Force Data Carrier Detect signal high.
	&C1	Let Data Carrier Detect follow carrier signal.
Command:	&Dn	Data Terminal Ready (DTR) Control
Values:		$n = 0, 1, 2,$ or 3
Default:		2
Description:	&D0	Modem ignores DTR signal.
	&D1	When DTR drops while in on-line data mode, the modem enters command mode, issues an OK, and remains connected.
	&D2	When DTR drops while in on-line data mode, the modem hangs up.
	&D3	When DTR drops, the modem hangs up and resets as if an ATZ command were issued.
Command:	&Fn	Load Factory Default Settings
Values:		$n = 0$
Default:		None
Description:	&F0	Load factory settings as active configuration.
Command:	&Gn	V.22bis Guard Tone Control
Values:		$n = 0, 1,$ or 2
Default:		0
Description:	&G0	Disable guard tone.
	&G1	Enable 550 Hz guard tone.
	&G2	Enable 1800 Hz guard tone.

☒: The **&G** command is not used in North America.

Command:	&Jn	Auxiliary Relay Control
Values:		$n = 0$
Default:		0
Description:	&J0	The auxiliary relay is never closed.
	&J1	Not supported—responds ERROR.
Command:	&Kn	Local Flow Control Selection
Values:		$n = 0, 3,$ or 4
Defaults:		3
Description:	&K0	Flow control disabled.
	&K3	Enable CTS/RTS hardware flow control.
	&K4	Enable XON/XOFF software flow control.

Command: &Mn Communications ModeValues: $n = 0$

Defaults: 0

Description: &M0 Asynchronous mode.
&M1 Reserved—responds ERROR.**Command: &Qn Asynchronous Communications Mode**Values: $n = 0, 5, \text{ or } 6$

Defaults: 5

Description: &Q0 Asynchronous with data buffering. Same as **W0**.
&Q5 Error control with data buffering. Same as **W3**.
&Q6 Asynchronous with data buffering. Same as **W0**.**Command: &Sn Data Set Ready (DSR) Control**Values: $n = 0 \text{ or } 1$

Default: 0

Description: &S0 Force DSR high (on).
&S1 Let DSR follow CD.**Command: &Tn Self-Test Commands**Values: $n = 0, 1, 3 \text{ or } 6$

Default: None

Description: &T0 Abort. Stop any test in progress.
&T1 Local analog loop test.
&T3 Local digital loopback test.
&T6 Remote digital loopback test.**Command: &V View Current Configuration**

Values: n/a

Description: Displays the active modem settings.

Command: &Wn Store Current ConfigurationValues: $n = 0$

Default: None

Description: &W0 Store active modem settings in NVRAM; load them at power-on or following the **ATZ** command instead of loading the factory defaults from ROM.**Command: &Yn Select Stored Configuration for Hard Reset**Values: $n = 0$

Default: 0

Description: &Y0 Select stored configuration 0 on power-up. (For backward compatibility with some software.)
&Y1 Not supported—responds ERROR.**Command: &Zn=x Store Telephone Number**Values: $n = 0, 1, 2, \text{ or } 3$
 $x = \text{Dialing string}$

Default: None

Description: Stores telephone dial string x in memory location n . Dial the stored number using the command **ATDS=n**.**Command: \Gn Modem Port Flow Control**Values: $n = 0$

Default: 0

Description: \G0 Returns an *OK* for backward compatibility with some software.
\G1 Not supported—responds ERROR.**Command: \Jn Data Buffer Control**Values: $n = 0$

Default: 0

Description: \J0 Enable data buffer—serial port speed is independent of connect speed.
\J1 Not supported—responds ERROR.

Command:	\Kn	Set Break Control
Values:		$n = 5$
Default:		5
Description:	\K5	Modem sends break signal received from the DTE to the remote modem.
Command:	\Nn	Error Correction Mode Selection
Values:		$n = 0-5$, or 7
Default:		3
Description:	\N0	Non-error correction mode with data buffering (same as &Q6).
	\N1	Direct mode.
	\N2	MNP reliable mode.
	\N3	V.42/MNP auto-reliable mode.
	\N4	V.42 reliable mode.
	\N5	V.42, MNP, or non-error correction (same as W3).
	\N7	V.42, MNP, or non-error correction (same as W3).
Command:	\Qn	Local Flow Control Selection
Values:		$n = 0, 1$, or 3
Default:		3
Description:	\Q0	Disable flow control (same as &K0).
	\Q1	XON/XOFF software flow control (same as &K4).
	\Q2	CTS-only flow control. Not supported—responds ERROR.
	\Q3	RTS/CTS hardware flow control (same as &K3).
Command:	\Tn	Inactivity Timer
Values:		$n = 0-255$
Default:		n/a
Description:	\Tn	Inactivity timer setting contingent on either \T value or S-Register S30 value (e.g., AT\T45&W0<cr> configures in parallel ATS30=45&W0<cr>), and vice versa.
Command:	\Vn	Protocol Result Code
Values:		$n = 0$ or 1
Default:		1
Description:	\V0	Disable protocol result code appended to DCE speed.
	\V1	Enable protocol result code appended to DCE speed.
Command:	\Xn	XON/XOFF Pass-Through
Values:		$n = 0$ or 1
Defaults:		0
Description:	\X0	Respond to and discard XON/XOFF characters.
	\X1	Not supported—responds ERROR.
Command:	-Cn	Data Calling Tone
Values:		$n = 0$ or 1
Defaults:		0
Description:	-C0	Disable V.25 data calling tone.
	-C1	Enable V.25 data calling tone.
Command:	%B	View Numbers in Blacklist
Values:		n/a
Description:		If blacklisting is in effect, this command displays the numbers for which the last call attempted in the previous two hours failed. In countries that do not require blacklisting, the ERROR result code appears.
Command:	%Cn	Data Compression Control
Values:		$n = 0$ or 1
Default:		1
Description:	%C0	Disable V.42bis/MNP 5 data compression.
	%C1	Enable V.42bis/MNP 5 data compression.

Command: **+ES=6 Enable Synchronous Buffered Mode**

Values: n/a

Description: Allows an H.324 video application direct access to the synchronous data channel. On underflow, the modem sends HDLC flag idle (0x7E) to the remote modem. This special error correction mode is overridden by any of the following commands: **&F**, **&M**, **&Q**, and **W**. **+ES = ?** shows the only allowed value.

Command: **&&S Speaker Codec Loopback**

Values: n/a

Description: Provides a loopback from the microphone to the speaker. *For testing and debugging only.*

Command: **%T94 Testing External RAM**

Values: n/a

Description: This command is used for testing the external RAM. Enter AT%T94<cr> to determine the status of external RAM. The response you should receive will be either "FAIL" or "PASS"

Command: **%T125 Testing DSP 56K Code Version/Checksum**

Values: n/a

Description: Entering AT%T125<cr> tests the DSP56K code version and checksum running in external RAM. Upon issuing this command the user may then issue ATi4<cr> to get DSP version or ATi1<cr> to get DSP checksum in RAM.

Entering AT%T124<cr> tests the DSP56K code version and checksum running in internal ROM. Upon issuing this command the user may then issue ATi4<cr> to get DSP version or ATi1<cr> to get DSP checksum in ROM.

Appendix E - TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) is a protocol suite and related applications developed for the U.S. Department of Defense in the 1970s and 1980s specifically to permit different types of computers to communicate and exchange information with one another. TCP/IP is currently mandated as an official U.S. Department of Defense protocol and is also widely used in the UNIX community.

Before you install TCP/IP on your network, you need to establish your Internet addressing strategy. First, choose a domain name for your company. A domain name is the unique Internet name, usually the name of your business, that identifies your company. For example, Multi-Tech's domain name is multitech.com (where .com indicates this is a commercial organization; .edu denotes educational organizations, .gov denotes government organizations). Next, determine how many IP addresses you'll need. This depends on how many individual network segments you have, and how many systems on each segment need to be connected to the Internet. You'll need an IP address for each network interface on each computer and hardware device.

IP addresses are 32 bits long and come in two types: network and host. Network addresses come in five classes: A, B, C, D, and E. Each class of network address is allocated a certain number of host addresses. For example, a class B network can have a maximum of 65,534 hosts, while a class C network can have only 254. The class A and B addresses have been exhausted, and the class D and E addresses are reserved for special use. Consequently, companies now seeking an Internet connection are limited to class C addresses.

Early IP implementations ran on hosts commonly interconnected by Ethernet local area networks (LAN). Every transmission on the LAN contains the local network, or medium access control (MAC), address of the source and destination nodes. The MAC address is 48-bits in length and is non-hierarchical; MAC addresses are never the same as IP addresses.

When a host needs to send a datagram to another host on the same network, the sending application must know both the IP and MAC addresses of the intended receiver. Unfortunately, the IP process may not know the MAC address of the receiver. The Address Resolution Protocol (ARP), described in RFC 826 (located at <ftp://ds.internic.net/rfc/rfc826.txt>) provides a mechanism for a host to determine a receiver's MAC address from the IP address. In the process, the host sends an ARP packet in a frame containing the MAC broadcast address; and then the ARP request advertises the destination IP address and asks for the associated MAC address. The station on the LAN that recognizes its own IP address will send an ARP response with its own MAC address. An ARP message is carried directly in an IP datagram.

Other address resolution procedures have also been defined, including those which allow a diskless processor to determine its IP address from its MAC address (Reverse ARP, or RARP), provides a mapping between an IP address and a frame relay virtual circuit identifier (Inverse ARP, or InARP), and provides a mapping between an IP address and ATM virtual path/channel identifiers (ATMARP).

The TCP/IP protocol suite comprises two protocols that correspond roughly to the OSI Transport and Session Layers; these protocols are called the Transmission Control Protocol and the User Datagram Protocol (UDP). Individual applications are referred to by a port identifier in TCP/UDP messages. The port identifier and IP address together form a "socket". Well-known port numbers on the server side of a connection include 20 (FTP data transfer), 21 (FTP control), 23 (Telnet), 25 (SMTP), 43 (whois), 70 (Gopher), 79 (finger), and 80 (HTTP).

TCP, described in RFC 793 (<ftp://ds.internic.net/rfc/rfc793.txt>) provides a virtual circuit (connection-oriented) communication service across the network. TCP includes rules for formatting messages, establishing and terminating virtual circuits, sequencing, flow control, and error correction. Most of the applications in the TCP/IP suite operate over the "reliable" transport service provided by TCP.

UDP, described in RFC 768 (<ftp://ds.internic.net/rfc/rfc768.txt>) provides an end-to-end datagram (connectionless) service. Some applications, such as those that involve a simple query and response, are better suited to the datagram service of UDP because there is no time lost to virtual

circuit establishment and termination. UDP's primary function is to add a port number to the IP address to provide a socket for the application.

The Application Layer protocols are examples of common TCP/IP applications and utilities, which include:

- Telnet (Telecommunication Network): a virtual terminal protocol allowing a user logged on to one TCP/IP host to access other hosts on the network, described in RFC 854 (<ftp://ds.internic.net/rfc/rfc854.txt>).
- FTP: the File Transfer Protocol allows a user to transfer files between local and remote host computers per IETF RFC 959 (<ftp://ds.internic.net/rfc/rfc959.txt>).
- Archie: a utility that allows a user to search all registered anonymous FTP sites for files on a specified topic.
- Gopher: a tool that allows users to search through data repositories using a menu-driven, hierarchical interface, with links to other sites, per RFC 1436 (<ftp://ds.internic.net/rfc/rfc1436.txt>).
- SMTP: the Simple Mail Transfer Protocol is the standard protocol for the exchange of electronic mail over the Internet, per IETF RFC 821 (<ftp://ds.internic.net/rfc/rfc821.txt>).
- HTTP: the Hypertext Transfer Protocol is the basis for exchange of information over the World Wide Web (WWW). Various versions of HTTP are in use over the Internet, with HTTP version 1.0 (per RFC 1945) (<ftp://ds.internic.net/rfc/rfc1945.txt>) being the most current.
- HTML: WWW pages are written in the Hypertext Markup Language (HTML), an ASCII-based, platform-independent formatting language, per IETF RFC 1866 (<ftp://ds.internic.net/rfc/rfc1866.txt>).
- Finger: used to determine the status of other hosts and/or users, per IETF RFC 1288 (<ftp://ds.internic.net/rfc/rfc1288.txt>).
- POP: the Post Office Protocol defines a simple interface between a user's mail reader software and an electronic mail server; the current version is POP3, described in IETF RFC 1460 (<ftp://ds.internic.net/rfc/rfc1460.txt>).
- DNS: the Domain Name System defines the structure of Internet names and their association with IP addresses, as well as the association of mail, name, and other servers with domains.
- SNMP: the Simple Network Management Protocol defines procedures and management information databases for managing TCP/IP-based network devices. SNMP, defined by RFC 1157 (<ftp://ds.internic.net/rfc/rfc1157.txt>) is widely deployed in local and wide area network. SNMP Version 2 (SNMPv2), per RFC 1441 (<ftp://ds.internic.net/rfc/rfc1441.txt>) adds security mechanisms that are missing in SNMP, but is also more complex.
- Ping: a utility that allows a user at one system to determine the status of other hosts and the latency in getting a message to that host. Ping uses ICMP Echo messages.
- Whois/NICNAME: Utilities that search databases for information about Internet domain and domain contact information, per RFC 954 (<ftp://ds.internic.net/rfc/rfc954.txt>).
- Traceroute: a tool that displays the route that packets will take when traveling to a remote host.

Internet Protocol (IP)

IP is the Internet standard protocol that tracks Internetwork node addresses, routes outgoing messages and recognizes incoming messages, allowing a message to cross multiple networks on the way to its final destination. The IPv6 Control Protocol (IPv6CP) is responsible for configuring, enabling, and disabling the IPv6 protocol modules on both ends of the point-to-point link. IPv6CP uses the same packet exchange mechanism as the Link Control Protocol (LCP). IPv6CP packets are not exchanged until PPP has reached the Network-Layer Protocol phase. IPv6CP packets received before this phase is reached are silently discarded. (See also TCP/IP.)

Before you install TCP/IP on your network, you need to establish your Internet addressing strategy. You first choose a domain name for your company. A domain name is the unique Internet name, usually the name of your business, that identifies your company. For example, Multi-Tech's domain name is multitech.com (where .com indicates this is a commercial organization; .edu denotes educational organizations, .gov denotes government organizations, etc.). Next, you determine how many IP addresses you'll need. This depends on how many individual network segments you have, and how many systems on each segment need to be connected to the Internet. You need an IP address for each network interface on each computer and hardware device.

IP addresses are 32 bits long and come in two types: network and host. Network addresses come in five classes: A, B, C, D, and E. Each class of network address is allocated a certain number of host addresses. For example, a class B network can have a maximum of 65,534 hosts, while a class C network can have only 254. The class A and B addresses have been exhausted, and the class D and E addresses are reserved for special use. Consequently, companies now seeking an Internet connection are limited to class C addresses. The current demand for Internet connections will exhaust the current stock of 32-bit IP addresses. In response, Internet architects have proposed the next generation of IP addresses, IPng (IP Next Generation). It will feature 16-byte (128-bit) addressing, surpassing the capacities of 32-bit IP. Still in its design phase, IPng (also known as IPv6) is not expected to be widely deployed before the end of this century.

An IP address can serve only a single physical network. Therefore, if your organization has multiple physical networks, you must make them appear as one to external users. This is done via "subnetting", a complex procedure best left to ISPs and others experienced in IP addressing. Since IP addresses and domain names have no inherent connection, they are mapped together in databases stored on Domain Name Servers (DNS). If you decide to let an Internet Service Provider (ISP) administer your DNS server, the ISP can assist you with the domain name and IP address assignment necessary to configure your company's site-specific system information. Domain names and IP addresses are granted by the InterNIC. To check the availability of a specific name or to obtain more information, call the InterNIC at (703)742-4777.



Glossary of Terms



A

Access: The T1 line element made up of two pairs of wire that the telephone company brings to the customer premises. The Access portion ends with a connection at the local telco (LEC or RBOC).

Accunet Spectrum of Digital Services (ASDS): The AT&T 56 Kbps leased (private) line service. Similar to services of MCI and Sprint. ASDS is available in nx56/64 Kbps, where n=1, 2, 4, 6, 8, 12.

ACK (ACKnowledgement code) (pronounced “ack”): A communications code sent from a receiving modem to a transmitting modem to indicate that it is ready to accept data. It is also used to acknowledge the error-free receipt of transmitted data. Contrast with NAK.

Adaptive Differential Pulse Code (ADCPM): In multimedia applications, a technique in which pulse code modulation samples are compressed before they are stored on a disk. ADCPM, an extension of the PCM format, is a standard encoding format for storing audio information in a digital format. It reduced storage requirements by storing differences between successive digital samples rather than full values.

Address: A numbered location inside a computer. It's how the computer accesses its resources, like a video card, serial ports, memory, etc.

AMI line coding: One of two common methods of T1 line coding (with B8ZS). AMI line coding places restrictions on user data (B8ZS does not).

Analog signal: A waveform which has amplitude, frequency and phase, and which takes on a range of values between its maximum and minimum points.

Analog Transmission: One of two types of telecommunications which uses an analog signal as a carrier of voice, data, video, etc. An analog signal becomes a carrier when it is modulated by altering its phase, amplitude and frequency to correspond with the source signal. Compare with digital transmission.

Application Program Interface (API): A software module created to allow dissimilar, or incompatible applications programs to transfer information over a communications link. APIs may be simple or complex; they are commonly required to link PC applications with mainframe programs.

ASCII (American Standard Code for Information Interchange) (pronounced “askey”): A binary code for data that is used in communications and in many computers and terminals. The code is used to represent numbers, letters, punctuation and control characters. The basic ASCII code is a 7-bit character set which defines 128 possible characters. The extended ASCII file provides 255 characters.

Asynchronous Transfer Mode (ATM): A very high-speed method of transmission that uses fixed-size cells of 53 bytes to transfer information over fiber; also known as cell relay.

AT Commands: A standard set of commands used to configure various modem parameters, establish connections and disconnect. The “AT” is used to get the “attention” of the modem before the actual command is issued.

Availability: The measure of the time during which a circuit is ready for use; the complement of circuit “outage” (100% minus % outage = % available).

B

B7ZS (Bipolar 7 Zero Suppression) line coding: One method of T1 line coding (see also “B8ZS” and “AMI”). B7ZS line coding does not place restrictions on user data (AMI does).

B8ZS (Bipolar 8 Zero Suppression) line coding: One of two common methods of T1 line coding (with AMI). B8ZS line coding does not place restrictions on user data (AMI does). A coding method used to produce 64 Kbps “clear” transmission. (See also “B7ZS” and “AMI” line coding)

Backbone: 1. A set of nodes and their interconnecting links providing the primary data path across a network. 2. In a local area network multiple-bridge ring configuration, a high-speed link to which the rings are connected by means of bridges. A backbone may be configured as a bus or as a ring. 3. In a wide area network, a high-speed link to which nodes or data switching exchanges (DSEs) are connected. 4. A common distribution core that provides all electrical power, gases, chemicals, and other services to the sectors of an automated wafer processing system.

Background: An activity that takes place in the PC while you are running another application. In other words, the active user interface does not correspond to the ‘background’ task.

Bandwidth: The transmission capacity of a computer channel, communications line or bus. It is expressed in cycles per second (hertz), the bandwidth being the difference between the lowest and highest frequencies transmitted. The range of usable frequencies that a transmission medium will pass without unacceptable attenuation or distortion. Bandwidth is a factor in determining the amount of information and the speed at which a medium can transmit data or other information.

Backward Explicit Congestion Notification (BECN): A bit that tells you that a certain frame on a particular logical connection has encountered heavy traffic. The bit provides notification that congestion-avoidance procedures should be initiated in the opposite direction of the received frame. See also FECN (Forward Explicit Congestion Notification).

Basic Rate Interface (BRI): An ISDN access interface type comprised of two B-channels each at 64 Kbps and one D-channel at 64 Kbps (2B+D).

Bell Operating Companies (BOC): The family of corporations created during the divestiture of AT&T. BOCs are independent companies which service a specific region of the US. Also called Regional Bell Operating Companies (RBOCs).

Bell Pub 41450: The Bell publication defining requirements for data format conversion, line conditioning, and termination for direct DDS connection.

Bell Pub 62310: The Bell publication defining requirements for data format conversion, line conditioning, and termination for direct DDS connection.

Binary Synchronous Communication (BSC): A form of telecommunication line control that uses a standard set of transmission control characters and control character sequences, for binary synchronous transmission of binary-coded data between stations.

Bit (Binary digit): A bit is the basis of the binary number system. It can take the value of 1 or 0. Bits are generally recognized as the electrical charge generated or stored by a computer that represent some portion of usable information.

Bit Error Rate Test (BERT): A device or routine that measures the quality of data transmission. A known bit pattern is transmitted, and the errors received are counted and a BER (bit error rate) is calculated. The BER is the ratio of received bits in error relative to the total number of bits received, expressed in a power of 10.

Bit robbing: The use of the least significant bit per channel in every sixth frame for signaling. The line signal bits "robbed" from the speech part conveys sufficient pre-ISDN telephony signaling information with the remaining line signal bits providing sufficient line signaling bits for recreating the original sound. See "robbed bit signaling".

Blue Alarm: An error indication signal consisting of all 1s indicating disconnection or attached device failure. Contrast "Red Alarm" and "Yellow Alarm".

Bps (bits per second): A unit to measure the speed at which data bits can be transmitted or received. Bps differs from baud when more than one bit is represented by a single cycle of the carrier.

Bridges: 1. A functional unit that interconnects two local area networks that use the same logical link protocol but may use different medium access control protocols. 2. A functional unit that interconnects multiple LANs (locally or remotely) that use the same logical link control protocol but that can use different medium access control protocols. A bridge forwards a frame to another bridge based on the medium access control (MAC) address. 3. In the connection of local loops, channels, or rings, the equipment and techniques used to match circuits and to facilitate accurate data transmission.

Buffer: A temporary storage register or Random Access Memory (RAM) used in all aspects of data communications which prevents data from being lost due to differences in transmission speed. Keyboards, serial ports, muxes and printers are a few examples of the devices that contain buffers.

Bus: A common channel between hardware devices either internally between components in a computer, or externally between stations in a communications network.

Byte: The unit of information a computer can handle at one time. The most common understanding is that a byte consists of 8 binary digits (bits), because that's what computers can handle. A byte holds the equivalent of a single character (such as the letter A).

C

Call Setup Time: The time to establish a circuit-switched call between two points. Includes dialing, wait time, and CO/long distance service movement time.

Carrier Group Alarm (CGA): A T1 service alarm generated by a channel bank when an OOF condition occurs for a predefined length of time (usually 300mS to 2.5 seconds). The CGA causes the calls using a trunk to be dropped and for trunk conditioning to be applied.

Carrier signal: An analog signal with known frequency, amplitude and phase characteristics used as a transport facility for useful information. By knowing the original characteristics, a receiver can interpret any changes as modulations, and thereby recover the information.

CCITT (Consultative Committee for International Telephone and Telegraph): An advisory committee created and controlled by the United Nations and headquartered in Geneva whose purpose is to develop and to publish recommendations for worldwide standardization of telecommunications devices. CCITT has developed modem standards that are adapted primarily by PTT (post, telephone and telegraph) organizations that operate telephone networks of countries outside of the U.S. See also ITU.

Central Office (CO): The lowest, or most basic level of switching in the PSTN (public switched telephone network). A business PABX or any residential telephone connects to the PSTN at a central office.

Centrex: A multi-line service offered by operating telcos which provides, from the telco CO, functions and features comparable to those of a PBX for large business users. See also "Private Branch Exchange", "Exchange".

Channel: A data communications path between two computer devices. Can refer to a physical medium (e.g., UTP or coax), or to a specific carrier frequency.

Channel Bank: A device that acts as a converter, taking the digital signal from the T1 line into a phone system and converting it to the analog signals used by the phone system. A channel bank acts as a multiplexer, placing many low-speed voice or data transactions on a single high-speed link.

CHAP (Challenge-Handshake Authentication Protocol): An authentication method that can be used when connecting to an Internet Service Provider. CHAP allows you to log in to your provider automatically, without the need for a terminal screen. It is more secure than Password Authentication Protocol (See PAP) since it does not send passwords in text format.

Circuit-switched Network: A technology used by the PSTN that allocates a pair of conductors for the exclusive use of one communication path. Circuit switching allows multiple conversations on one talk path only if the end-users multiplex the signals prior to transmission.

Circuit Switching: The temporary connection of two or more communications channels using a fixed, non-shareable path through the network. Users have full use of the circuit until the connection is terminated.

Clear Channel: A transmission path where the full bandwidth is used (i.e., no bandwidth needed for signaling, carrier framing or control bits). A 64 Kbps digital circuit usually has 8 Kbps used for signaling. ISDN has two 64 Kbps circuits, and a 16 Kbps packet service of which part is used for signaling on the 64K channels.

Client-Server: In TCP/IP, the model of interaction in distributed data processing in which a program at one site sends a request to a program at another site and awaits a response. The requesting program is called a client; the answering program is called a server.

Cluster Controller: A device that can control the input/output operations of more than one device connected to it. A cluster controller may be controlled by a program stored and executed in the unit, or it may be entirely controlled by hardware.

Committed Burst Size: The maximum number of bits that the frame relay network agrees to transfer during any measurement interval.

Committed Information Rate (CIR): An agreement a customer makes to use a certain minimum data transmission rate (in bps). The CIR is part of the frame relay service monthly billing, along with actual usage, that users pay to their frame relay service provider.

Compression: 1. The process of eliminating gaps, empty fields, redundancies, and unnecessary data to shorten the length of records or blocks. 2. In SNA, the replacement of a string of up to 64-repeated characters by an encoded control byte to reduce the length of the data stream to the LU-LU session partner. The encoded control byte is followed by the character that was repeated (unless that character is the prime compression character). 3. In Data Facility Hierarchical Storage Manager, the process of moving data instead of allocated space during migration and recall in order to release unused space. 4. Contrast with decompression.

COMx Port: A serial communications port on a PC.

congestion: A network condition where there is too much data traffic. The ITU I.233 standard defines congestion management in terms of speed and burstiness.

congestion notification: The function in frame relay that ensures that user data transmitted at a rate higher than the CIR are allowed to slow down to the rate of the available network bandwidth.

Consecutive Severely Errored Seconds (CSES): An error condition that occurs when from 3 to 9 SES (Severely Errored Seconds) are logged consecutively.

Customer Premise Equipment (CPE): The generic term for data comm and/or terminal equipment that resides at the user site and is owned by the user with the following exclusions: Over voltage protection equipment, inside wiring, coin operated or pay telephones, "company-official" equipment, mobile telephone equipment, "911" equipment, equipment necessary for the provision of communications for national defense, or multiplexing equipment used to deliver multiple channels to the customer.

D

D4: the T1 4th generation channel bank.

D4 channelization: Refers to the compliance with AT&T TR 62411 for DS1 frame layout.

D4 framing: The T1 format for framing in AT&T D-Series channel banks, in which there are 12 separate 193-bit frames in a super-frame. A D4 framing bit is used to identify the channel and the signaling frame. Signalling for voice channels is carried in-band for every channel, along with the encoded voice. See "robbed-bit signaling".

Data Communications Equipment (DCE): Any device which serves as the portal of entry from the user equipment to a telecommunications facility. A modem is a DCE for the telephone network (PSTN) that is commonly on site at the user's premises. Packet Switched Networks have another level of DCE which is most often located at a central office.

Data Link Connection Identifier (DLCI): One of the six components of a frame relay frame. Its purpose is to distinguish separate virtual circuits across each access connection. Data coming into a frame relay node is thus allowed to be sent across the interface to the specified "address". The DLCI is confirmed and relayed to its destination, or if the specification is in error, the frame is discarded.

Data Terminal Ready (DTR): A control signal sent from the DTE to the DCE that indicates that the DTE is powered on and ready to communicate.

Dataphone Digital Service (DDS): A private line digital service that offers 2400, 4800, 9600 and 56 Kbps data rates on an inter-LATA basis by AT&T and on an intra-LATA basis by the BOCs.

Data Service Unit (DSU): A device that provides a digital data service interface directly to the data terminal equipment. The DSU provides loop equalization, remote and local testing capabilities, and a standard EIA/CCITT interface.

Dedicated Line: A communication line that is not switched. The term leased line is more common.

Default: This is a preset value or option in software packages, or in hardware configuration, that is used unless you specify otherwise.

Device driver: Software that controls how a computer communicates with a device, such as a printer or mouse.

Digital Cross-connect System (DCS): The CO device which splits and redistributes the T1 bandwidth. the DCS takes time slots from various T1 lines and alters them to provide the needed connectivity. DCS connections are made with software at an administrator's workstation.

Digital Data: Information represented by discrete values or conditions (contrast "Analog Data").

Digital Loopback: A technique used for testing the circuitry of a communications device. Can be initiated locally, or remotely (via a telecommunications device). The tested device decodes and encodes a received test message, then echoes the message back. The results are compared with the original message to determine if corruption occurred en route.

Digital PBX: A Private Branch Exchange that operates internally on digital signals. See also "Exchange".

Digital Service, level 0 (DS0): The world-wide standard speed (64 Kbps) for digital voice conversation using PCM (pulse coded modulation).

Digital Service, level 1 (DS1): The 1.544M bps voice standard (derived from an older Bell System standard) for digitized voice transmission in North America. The 1.544M bps consists of 24 digitally-encoded 64 Kbps voice channels (north America) and 2.048M bps (30 channels) elsewhere.

Digital Signal: A discrete or discontinuous signal (e.g., a sequence of voltage pulses). Digital devices, such as terminals and computers, transmit data as a series of electrical pulses which have discrete jumps rather than gradual changes.

Digital Signaling Rates (DSn): A hierarchical system for transmission rates, where "DS0" is 64 Kbps (equivalent to ISDN B channel), and DS1 is 1.5 Mbps (equivalent to ISDN PRI).

Digital Transmission: A method of electronic information transmission common between computers and other digital devices. Analog signals are waveforms: a combination of many possible voltages. A computer's digital signal may be only "high" or "low" at any given time. Therefore, digital signals may be "cleaned up" (noise and distortion removed) and amplified during transmission.

Digitize: To convert an analog signal to a digital signal.

DIP switch (pronounced "dip switch"): A set of tiny toggle switches, built into a DIP (dual in-line package), used for setting configurable parameters on a PCB (printed circuit board).

Domain Name Server (DNS): Also known as "resolvers", are a system of computers which convert domain names into IP addresses, which consist of a string of four numbers up to three digits each. Each applicant for a domain name must provide both a primary and a secondary DNS server; a domain name which fails to provide both primary and secondary DNS servers is known as a "lame delegation."

Driver: A software module that interfaces between the Operating System and a specific hardware device (e.g., color monitors, printers, hard disks, etc.). Also known as a device driver.

Drop and Insert: The process where a portion of information carried in a transmission system is demodulated ("Dropped") at an intermediate point and different information is included ("Inserted") for subsequent transmission.

DTE (Data Terminal Equipment): A term used to include any device in a network which generates, stores or displays user information. DTE is a telecommunications term which usually refers to PCs, terminals, printers, etc.

DTMF (Dual-Tone MultiFrequency): A generic push-button concept made popular by AT&T TouchTone.

Dynamic Host Configuration Protocol (DHCP): An IETF protocol which allows a server to dynamically assign IP addresses to Nodes (workstations). DHCP supports manual, automatic and dynamic address assignment; provides client information including the subnet mask, gateway address; and is routable. A DHCP server, generally a dedicated server, verifies the device's identity, "leases" an IP address for a predetermined period of time and reclaims the address upon expiration for reassignment to another workstation.

E

E&M: A telephony trunking system used for either switch-to-switch, or switch-to-network, or computer/telephone system-to-switch connection.

EIA: The Electronics Industries Association is a trade organization in Washington, DC that sets standards for use of its member companies. (See RS-232, RS-422, RS530.)

Encapsulation: A technique used by network-layer protocols in which a layer adds header information to the protocol data unit from the preceding layer. Also used in "enveloping" one protocol inside another for transmission. For example, IP inside IPX.

Errored Seconds (ES): Any second of operation that all 1.544M bits are not received exactly as transmitted. Contrast "Error Free Seconds".

Error Free Seconds (EFS): Any second of operation that all 1.544M bits are received exactly as transmitted. Contrast "Errored Seconds".

ESF Error Event: A T1 error condition that is logged when a CRC-6 error or an Out-Of-Frame (OOF) error occurs.

Ethernet: A 10-megabit baseband local area network that allows multiple stations to access the transmission medium at will without prior coordination, avoids contention by using carrier sense and deference, and resolves contention by using collision detection and transmission. Ethernet uses carrier sense multiple access with collision detection (CSMA/CD).

Excess Zeros: A T1 error condition that is logged when more than 15 consecutive 0s or fewer than one 1 bit in 16 bits occurs.

Exchange: A unit (public or private) that can consist of one or more central offices established to serve a specified area. An exchange typically has a single rate of charges (tariffs) that has previously been approved by a regulatory group.

Exchange Area: A geographical area with a single uniform set of charges (tariffs), approved by a regulatory group, for telephone services. Calls between any two points within an exchange area are local calls. See also "Digital PBX", "PBX".

Exchange Termination (ET): The carrier's local exchange switch. Contrast with "Loop Termination - LT".

Explicit Congestion Management: The method used in frame relay to notify the terminal equipment that the network is overly busy. The use of FECN and BECN is called explicit congestion management. Some end-to-end protocols use FECN or BECN, but usually not both options together. With this method, a congestion condition is identified and fixed before it becomes critical. Contrast with "implicit congestion".

Extended Super Frame (ESF): One of two popular formats for framing bits on a T1 line. ESF framing has a 24-frame super-frame, where robbed bit signaling is inserted in the LSB (bit 8 of the DS-0 byte) of frames 6, 12, 18 and 24. ESF has more T1 error measurement capabilities than D4 framing. Both ESF and B8ZS are typically offered to provide clear channel service.

F

Failed Seconds: A test parameter where the circuit is unavailable for one full second.

Failed Signal: A T1 test parameter logged when there are more than 9 SES (Severely Errored Seconds).

Fax (facsimile): Refers to the bit-mapped rendition of a graphics-oriented document (fax) or to the electronic transmission of the image over telephone lines (faxing). Fax transmission differs from data transmission in that the former is a bit-mapped approximation of a graphical document and, therefore, cannot be accurately interpreted according to any character code.

Firmware: A category of memory chips that hold their content without electrical power, they include ROM, PROM, EPROM and EEPROM technologies. Firmware becomes "hard software" when holding program code.

Foreground: The application program currently running on and in control of the PC screen and keyboard. The area of the screen that occupies the active window. Compare with "background".

Fractional T1 (FT1): A digital data transmission rate between 56 Kbps (DS0 rate) and 1.544M bps (the full T1 rate - in North America). FT1 is typically provided on 4-wire (two copper pairs) UTP. Often used for video conferencing, imaging and LAN interconnection due to its low cost and relatively high speed. FT1 rates are offered in 64 Kbps multiples, usually up to 768 Kbps.

Frequency: A characteristic of an electrical or electronic signal which describes the periodic recurrence of cycles. Frequency is inversely proportional to the wavelength or pulse width of the signal (i.e., long wavelength signals have low frequencies and short wavelength signals yield high frequencies).

Foreign Exchange (FX): A CO trunk with access to a distant CO, allowing ease of access and flat-rate calls anywhere in the foreign exchange area.

Foreign Exchange Office (FXO): provides local telephone service from a CO outside of ("foreign" to) the subscriber's exchange area. In simple form, a user can pick up the phone in one city and receive a tone in the foreign city. Connecting a POTS telephone to a computer telephony system via a T1 link requires a channel bank configured for the FX connection. To generate a call from the POTS set to the computer telephony system, a FXO connection must be configured.

Foreign Exchange Station (FXS): See FX, FXO. To generate a call from the computer telephony system to the POTS set, an FXS connection must be configured.

Forward Explicit Congestion Notification (FECN): A bit that tells you that a certain frame on a particular logical connection has encountered heavy traffic. The bit provides notification that congestion-avoidance procedures should be initiated in the same direction of the received frame. See also BECN (Backward Explicit Congestion Notification).

Frame: A group of data bits in a specific format to help network equipment recognize what the bits mean and how to process them. The bits are sent serially, with a flag at each end signifying the start and end of the frame.

Frame Relay: A form of packet switching that uses small packets and that requires less error checking than other forms of packet switching. Frame relay is effective for sending "bursty" data at high speeds (56/64K, 256K, and 1024 Kbps) over wide area networks. Frame Relay specifications are defined by ANSI documents ANSI T1.602, T1.606, T1S1/90-175, T1S1/90-213, and T1S1/90-214. In using frame relay, blocks of information (frames) are passed across a digital network interface using a "connection number" that is applied to each frame to distinguish between individual frames.

Frame Relay Forum: A non-profit organization of 300+ vendors and service providers, based in Foster City, CA, that are developing and deploying frame relay equipment.

Frame Relay Implementors Forum: A group of companies supporting a common specification for frame relay connection to link customer premises equipment to telco network equipment. Their specification supports ANSI frame relay specs and defines extensions such as local management.

Frame Relay Access Device (FRAD): A piece of equipment that acts as a concentrator or frame assembler/dissassembler that can support multiple protocols and provide basic "routing" functions.

G

Gateway: 1. A functional unit that interconnects two computer networks with different network architectures. A gateway connects networks or systems of different architectures. A bridge interconnects networks or systems with the same or similar architectures. 2. A network that connects hosts.

Graphical User Interface (GUI): A type of computer interface consisting of a visual metaphor of a real-world scene, often of a desktop. Within that scene are icons, representing actual objects, that the user can access and manipulate with a pointing device.

H

Handshaking: A process that two modems go through at the time of call setup to establish synchronization over the data communications link. It is a synchronization and negotiation process accomplished by the exchange of predefined, mutually recognized control codes.

Hexadecimal: A base 16 numbering system used to represent binary values. Hex uses the numbers 0-9 and the letters A-F: usually notated by an "h" (e.g., "4CF h", read "four charley fox, hex"). The result is that one hex digit represents a 4-bit value.

High-level Data Link Control (HDLC): An ISO standard, bit-oriented data communications protocol that provides nearly error-free data transfers.

I

Implicit congestion management: A method of informing the terminal that the network is busy. This method relies on the end-system protocol to detect and fix the congestion problem. (TCP/IP is an example of a protocol using only implicit congestion management.) See also "explicit congestion management".

In-band: Refers to the type of signalling over the conversion path on an ISDN call. Contrast "out-of-band".

Insufficient Ones: A T1 error condition that is logged when fewer than one 1 in 16 0s or less than 12.5 % average 1s density is received.

Inter Exchange Carrier (IEC): The long distance company (LE) who's central office provides the point of reference for T1 access. Any common carrier authorized by the FCC to carry customer transmissions between LATAs.

Internet: Refers to the computer network of many millions of university, government and private users around the world. Each user has a unique Internet Address.

Internet Address (IP Address): A unique 32-bit address for a specific TCP/IP host on a network. Normally printed in dotted decimal format (e.g., 129.128.44.227).

Internet Protocol (IP): A protocol used to route data from its source to its destination in an Internet environment. The Internet Protocol was designed to connect local area networks. Although there are many protocols that do this, IP refers to the global system of interconnecting computers. It is a highly distributed protocol (each machine only worries about sending data to the next step in the route).

Internetwork Packet Exchange (IPX): A NetWare communications protocol used to route messages from one node to another. IPX packets include network addresses and can be routed from one network to another. An IPX packet can occasionally get lost when crossing networks, thus IPX does not guarantee delivery of a complete message. Either the application has to provide that control, or NetWare's SPX protocol must be used.

Interoperable: Devices from different vendors that can exchange information using a standard's base protocol.

I/O Addresses: Locations within the I/O address space of your computer used by a device, such as an expansion card, a serial port, or an internal modem. The address is used for communication between software and a device.

IRQ Level (Interrupt Request Level): The notification a processor receives when another portion of the computer's hardware requires its attention. IRQs are numbered so that the device issuing the IRQ can be identified, and so IRQs can be prioritized.

ISA (Industry Standards Architecture) (pronounced "ice a"): The classic 8 or 16-bit architecture introduced with IBM's PC-AT computer.

ISDN (Integrated Services Digital Network): An International telecommunications standard for transmitting voice, video and data over a digital communications line. ISDN is a world-wide telecommunications service that uses digital transmission and switching technology to support voice and digital data communications. Frame relay was partially based on ISDN's data link layer protocol (LAPD). Frame relay can be used to transmit across ISDN services offering circuit-switched connection at 64 Kbps and higher speeds. Contrast Public Switched Telephone Network (PSTN).

ITU-TSS (formerly CCITT): International Telecommunications Union-Telecommunications Sector; the United Nations organization that prepares standards ("Recommendations") for resolving communications issues and problems.

J

No Entries.

K

Key Telephone System (KTS): Phone devices with multiple buttons that let you select incoming or outgoing CO phone lines directly. Similar in operation to a PBX, except with a KTS you don't have to dial a "9" for a call outside the building.

Key Service Unit (KSU): A small device containing the switching electronics for a business key telephone system (KTS).

Key Set: A telephone set with several buttons for call holding, line pickup, intercom, autodialing, etc. Also called a touchtone phone (Ericsson) and a KTS (Key Telephone Set).

L

LAPB: Link Access Procedure Balanced; based on the X.25 Layer 2 specification. A full-duplex point-to-point, bit-synchronous protocol commonly used as a data link control protocol to interface X.25 DTEs. LAPB is the link initialization procedure that establishes and maintains communications between the DTE and the DCE.

LAPD: Link Access Protocol for the D-Channel; based on the ISDN Q.921 specification. A full-duplex, point-to-point bit-synchronous link-level protocol for ISDN connections; different from LAPB in its framing sequence. Transmission is in units called "frames", and a frame may contain one or more X.25 packets.

Line Coding: The representation of 1s and 0s on a T1 line. The two methods of line coding commonly used, B8ZS and AMI, differ in the restrictions placed on user data. T1 line coding ensures that sufficient timing information is sent with the digital signal to ensure recovery of all the bits at the far end. Timing information on the T1 line is included in the form of 1s in the data stream; a long string of 0s in the data stream could cause problems recovering the data.

Line Termination (LT): The electronics at the ISDN network side of the user/network interface that complements the NT1 at the user side. The LT and the NT1 together provide the high-speed digital line signals required for BRI access.

Listed Directory Number (LDN): The main number assigned by the telco; the number listed in the telephone directory and also provided by Directory Assistance. Some devices can have more than one LDN, such as ISDN devices that have one LDN for voice and another LDN for data.

Local Area Network (LAN): 1. A computer network located on a user's premises within a limited geographical area. Communication within a local area network is not subject to external regulations; however, communication across the LAN boundary may be subject to some form of regulation. 2. A LAN does not use store-and-forward techniques. 3. A network in which a set of devices are connected to one another for a communication and that can be connected to a larger network.

Local Access and Transport Area (LATA): A post-divestiture geographical area generally equivalent to a Standard Metropolitan Statistical Area. At divestiture, the territory served by the Bell system was divided into approximately 161 LATAs. The Bell Operating Companies (BOCs) provide Intra-LATA services.

Local Exchange Carrier (LEC): The local phone company which provides local (i.e., not long distance) transmission services. AKA "telco". LECs provide T1 or FT1 access to LDCs (unless the T1 circuit is completely intra-LATA). Inter-LATA T1 circuits are made up of a combination of Access and Long Haul facilities.

Local Management Interface (LMI): A specification for frame relay equipment that defines status information exchange.

Local Loop: A transmission path, typically twisted-pair wire, between an individual subscriber and the nearest public telecommunications network switching center. The wires provide ISDN service, but require an NT1 at the user end and an LT at the network end. (AKA, "loop" or "subscriber loop".)

Logical Link Control (LLC2): In a local area network, the protocol that governs the exchange of transmission frames between data stations independently of how the transmission medium is shared. The LLC2 protocol was developed by the IEEE 802 committee and is common to all LAN standards.

Logical Unit (LU): A type of network accessible unit that enables end users to gain access to network resources and communicate with each other.

Long Haul: The T1 element that connects to the Access portion of the long distance company's (LDC's) central office. The LDC is commonly called the point of presence (POP). Each LDC has a number of POPs, located throughout the country. The LDC is also called an IEC (Inter Exchange Carrier).

Long Haul Communications: The type of phone call reaching outside of a local exchange (LE).

M

Management Information Base (MIB): A database of network management information used by the Common Management Information Protocol (CMIP) and the Simple Network Management Protocol (SNMP).

Megacom: An AT&T service with a normal WATS line (typically T1) between the customer premise and the AT&T serving class 4 CO are the customer's responsibility.

MegaLink: BellSouth's leased T1 service.

Message: Associated with such terms as packet, frame, and segment. 1. In information theory, an ordered series of characters intended to convey information. 2. An assembly of characters and sometimes control codes that is transferred as an entry from an originator to one or more recipients.

Modem: A communications device that enables a computer to transmit information over a telephone line. It converts the computer's digital signals into analog signals to send over a telephone line and converts them back to digital signals at the receiving end. Modems can be internal and fit into an expansion slot, or external and connect to a serial port.

Multi-Link/PPP (ML/PPP): A 'bandwidth on demand' technology that allows one logical PPP connection to add additional channels (as in a second ISDN channel) when the bandwidth is needed (however the vendor defines that situation). It may also be used with leased lines when the total bandwidth needed exceeds the available line speed - a form of inverse muxing.

Multiplexer (Mux): 1. A device that takes several input signals and combines them into a single output signal in such a manner that each of the input signals can be recovered. 2. A device capable of interleaving the events of two or more activities or capable of distributing the events of an interleaved sequence to the respective activities. 3. Putting multiple signals on a single channel.

Multiprotocol: A device that can interoperate with devices utilizing different network protocols.

Multithreading: The ability of a software system to be able to handle more than one transaction concurrently. This is contrasted to the case where a single transaction is accepted and completely processed before the next transaction processing is started.

N

Nailed Connection: A permanent or dedicated circuit of a previously switched circuit or circuits.

Nailed-up Circuit: A semi-permanent circuit established through a circuit-switching facility for point-to-point connectivity.

NAK (Negative Acknowledgment): Communications code used to indicate that a message was not properly received, or that a terminal does not wish to transmit. Contrast with ACK.

Network: A group of computers connected by cables or other means and using software that enables them to share equipment, such as printers and disk drives to exchange information.

Node: Any point within a network which has been assigned an address.

O

Object-Oriented: A method for structuring programs as hierarchically organized classes describing the data and operations of objects that may interact with other objects.

Office Channel Unit - Data Port (OCU-DP): The CO channel bank used as the interface between the customer's DSU and the channel bank.

Off-hook: The condition of a device which has accessed a phone line (with or without using the line). In modem use, this is equivalent to a telephone handset being picked up. Dialing and transmission are allowed, but incoming calls are not answered. Contrast "on-hook".

Off Premise Extension (OPX): An extension or phone that terminates in a location other than that of the PBX. Commonly used to provide a corporate member with an extension of the PBX at home.

Ones Density: the measure of the number of logical 1s on a T1 line compared to a given total number of bits on that line; used for timing information in data recovery in AMI and B8ZS.

On-Hook: The condition of a device which has not accessed a phone line. In modem use, this is equivalent to a telephone handset that has not been picked up. In other words, it can receive an incoming call. Contrast "off-hook".

Open Shortest Path First (OSPF): A hierarchical Interior Gateway Protocol (IGP) routing algorithm for IP that is a proposed standard for the Internet. OSPF incorporates least-cost routing, equal-cost routing, and load balancing.

Outage: The measure of the time during which a circuit is not available for use due to service interrupt. Outage is the complement of circuit "availability" (100% minus % available = % outage).

Out-of-band: Signaling that is separated from the channel carrying the information (e.g., the voice/data/video signal is separate from the carrier signal). Dialing and various other "supervisory" signals are included in the signaling element. Contrast "In-band" signaling.

Out of Frame (OOF): A T1 alarm condition that is logged on the loss of 2, 3 or 4 of 5 consecutive FT framing bits.

P

Packet: 1. In data communication, a sequence of binary digits, including data and control signals, that is transmitted and switched as a composite whole. The data, control signals and, possibly, error control information are arranged in a specific format. 2. Synonymous with data frame. 3. In TCP/IP, the unit of data passed across the interface between the Internet layer and the link layer. A packet includes an IP header and data. A packet can be a complete IP datagram or a fragment of an IP diagram. 4. In X.25, a data transmission information unit. A group of data and control characters, transferred as a unit, determined by the process of transmission. Commonly used data field lengths in packets are 128 or 256 bytes. 5. The field structure and format defined in the CCITT X.25 recommendation.

Packet Assembler/Disassembler (PAD): Used by devices to communicate over X.25 networks by building or stripping X.25 information on or from a packet.

Packet Data: The information format ("packetized") used for packet-mode calls.

Packet Mode: Refers to the switching of chunks of information for different users using statistical multiplexing to send them over the same transmission facility.

Parity bit: An extra bit attached to each byte of synchronous data used to detect errors in transmission.

Password Authentication Protocol (PAP): PAP (and CHAP) are widely-used authentication methods for communicating between ProxyServers, both for reaching the Internet and for securing temporary WAN connections such as dial-backup lines. CHAP uses a three-way handshake process that, in concept, resembles a dial-back routine and uses encrypted passwords. With PAP, one ProxyServer connects to the other and sends a plain text login and password.

Permanent Virtual Circuit (PVC): A connection between two endpoints dedicated to a single user. In ISDN, PVCs are established by network administration and are held for as long as the user subscribes to the service.

Physical Unit (PU): The component that manages and monitors the resources (such as attached links and adjacent link stations) associated with a node, as requested by an SSCP via an SSCP-PU session. An SSCP activates a session with the physical unit in order to indirectly manage, through the PU, resources of the node such as attached links. This term applies to type 2.0, type 4, and type 5 nodes only.

Point of Presence (POP): The central office's end points of the long distance carriers.

Point-to-Point Protocol (PPP): A protocol that lets a PC user access TCP/IP (Internet member) using an ISDN terminal adapter or a high-speed modem over a standard telephone line.

Port: A location for input or output data exchange. Computers, muxes, etc. have ports for various purposes.

Primary Rate Interface (PRI): Used on ISDN. In North America, and Japan, PRI is one 64Kbps D channel and 23 B channels. Elsewhere, it is one D channel and 30 B channels.

Primitive: An abstract representation of interaction across the access points indicating that information is being passed between the service user and the service provider. The OSI Reference Model defines four types of primitives: Request, Indication, Response and Confirm.

Private Branch Exchange (PBX): A telephone exchange located on the customer's premises. The PBX provides a circuit switching facility for telephone extension lines within the building, and access to the public telephone network. See also "Exchange".

PROM (Programmable Read Only Memory - pronounced "prom"): A permanent memory chip that can be programmed or filled by the customer after by the manufacturer has set initial values. Contrast with ROM.

Protocol: 1. A set of semantic and syntactic rules that determines the behavior of functional units in achieving communication. 2. In Open Systems Interconnection architecture, a set of semantic and syntactic rules that determine the behavior of entities in the same layer in performing communication functions. 3. In SNA, the meanings of and the sequencing rules for requests and responses used for managing the network, transferring data, and synchronizing the states of network components. 4. Synonymous with line control discipline.

ProxyServer: A secure gateway that provides multiple LAN users with high performance Internet access by functioning as a TCP/IP proxy server that resides on the outer edge of a firewall.

PSTN (Public Switched Telephone Network): A worldwide public voice telephone network that is used as a telecommunications medium for the transmission of voice, data and other information.

Public Data Network (PDN): A packet-switched network that is available to the public for individual ("subscriber") use. Typically, controlled by a government or a national monopoly.

Public Switched Telephone Network (PSTN): The group of circuit-switching voice carriers, which are commonly used as analog data communications services.

Pulse Code Modulation (PCM): 1. In data communication, variation of a digital signal to represent information; for example, by means of pulse amplitude modulation (PAM), pulse duration modulation (PDM), or pulse position modulation (PPM). 2. Transmissions of analog information in digital form through sampling and encoding the samples with a fixed number of bits.

Pulse dialing: One of two methods of dialing a telephone, usually associated with rotary-dial phones. Compare with "tone dialing".

Q

Quantizing: The process of analog-to-digital conversion by assigning a range, from the contiguous analog values, to a discrete number.

R

Random Access Memory (RAM): A computer's primary workspace. All data must be stored in RAM (even for a short while), before software can use the processor to manipulate the data. Before a PC can do anything useful it must move programs from disk to RAM. When you turn it off, all information in RAM is lost.

Rate Enforcement: The concept in frame relay where frames sent faster than the CIR are to be carried only if the bandwidth is available, otherwise they are to be discarded. (The frame relay network assumes that anything exceeding the CIR is of low priority.) Rate enforcement makes sure that the network will not get so congested that it isn't able to meet the agreed on CIR.

Recognized Private Operating Agency (RPOA): A corporation, private or government-controlled, that provides telecommunications services. RPOAs, such as AT&T, participate as non-voting members in the CCITT.

Red Alarm: A T1 error condition generated when a local failure (e.g., loss of synchronization) exists for 2.5 seconds, causing a Carrier Group Alarm (CGA). See also "Blue Alarm" and "Yellow Alarm".

Request for Comment (RFC): A set of papers in which Internet standards (published and proposed), along with generally-accepted ideas, proposals, research results, etc. are published.

Ring Down Box: A device that emulates a CO by generating POTS calls for testing and product demos.

Ring Down Circuit: A tie line connecting phones where picking up one phone automatically rings another phone. A feature used for emergencies to alert the person at the other phone of the incoming call.

RJ-11: An industry standard interface used for connecting a telephone to a modular wall outlet; comes in 4-and 6-wire packages.

RJ-45: An 8-wire modular connector for voice and data circuits.

Robbed Bit Signaling: The popular T1 signaling mechanism where the A and B bits are sent by each side of the T1 termination and are "buried" in the voice data of each voice channel in the T1 circuit. Since the bits are "robbed" infrequently, voice quality remains relatively uncompromised. See "bit robbing". The robbed-bit signaling technique is used in D4 channel banks to convey signaling information. The eighth (least significant) bit of each of the 24 8-bit time slots is "robbed" every sixth frame to convey voice-related signaling information such as on-hook, off-hook, etc, for each channel.

Router: A device that connects two networks using the same networking protocol. It operates at the Network Layer (Layer 3) of the OSI model for forwarding decisions.

Routing Information Protocol (RIP): A distance vector-based protocol that provides a measure of distance, or hops, from a transmitting workstation to a receiving workstation.

RS232-C: An EIA standard for a serial interface between computers and peripheral devices (modem, mouse, etc.). It uses a 25-pin DB-25, or a 9-pin DB-9 connector. The RS-232 standard defines the purposes, electrical characteristics and timing of the signals for each of the 25 lines.

RS-422: The EIA standard for a balanced interface with no accompanying physical connector. RS-422 products can use screw terminals, DB9, various DB25, and DB37 connectors.

RS-530: The EIA standard for the mechanical/electrical interface between DCEs and DTEs transmitting synchronous or asynchronous serial binary data. RS-530 provides for high data rates with the same connector used for RS-232; however, it is incompatible with RS-232.

S

Serial Port: The connector on a PC used to attach serial devices (those that need to receive data one bit after another), such as a mouse, a printer or a modem. This consists of a 9- or 25-pin connector that sends data in sequence (bit by bit). Serial ports are referred to as "COMx" ports, where x is 1 to 4 (i.e., COM1 through COM4). A serial port contains a conversion chip called a "UART" which translates between internal parallel and external serial formats.

Service: The requirements offered by an RPOA to its customers to satisfy specific telecommunications needs.

Serial Line Internet Protocol (SLIP): An Internet protocol which is used to run IP over serial lines such as telephone circuits.

Severely Errored Seconds (SES): Refers to a typical T1 error event where an error burst occurs (a short term, high bit-error rate that is self-clearing). Per the ITU-T (CCITT) G.821: any second in which the BER is less than 1×10^{-3} .

Signaling: The process of establishing, maintaining, accounting for, and terminating a connection between two endpoints (e.g., the user premises and the telco CO). Central office signals to the user premises can include ringing, dial tone, speech signals, etc. Signals from the user's telephone can include off-hook, dialing, speech to far-end party, and on-hook signals. In-band signaling techniques include pulse and tone dialing. With common channel signaling, information is carried out-of-band.

Simple Network Management Protocol (SNMP): TCP/IP protocol that allows network management.

Simultaneous Voice Data (SVD): A technology for letting a user send data via a modem, and use a handset to talk to another user at the same time over the same connection. The alternative, making a second call, can be expensive or even impossible. The uses for SVD are telecommuting, videoconferencing, distant learning, tech support, etc.

Stop Bit: One of the variables used for timing in asynchronous data transmission. Depending on the devices, each character may be trailed by 1, 1.5, or 2 stop bits.

Superframe (D4): A T1 transmission format that consists of 12 DS1 frames, or 2316 bits. A DS1 frame consists of 193 bit positions. A frame overhead bit is in the first position, and it is used for frame and signaling phase alignment only.

Subscriber Loop: See "Local loop".

Switched 56: A circuit-switched (full duplex digital synchronous data transmission) service that lets you dial a number and transmit data to it at 56 Kbps. It is a relatively low cost service, widely used in North America for telecommuting, videoconferencing and high speed data transfers. Many phone companies are (or will be) phasing out Switched 56 in favor of ISDN service.

Switched Virtual Circuit (SVC): A type of data transmission where the connection is maintained only until the call is cleared.

Switched Line: In communications, a physical channel established by dynamically connecting one or more discrete segments. This connection lasts for the duration of the call after which each segment can be used as part of a different channel. Contrast with leased line.

Switched Network: A network in which a temporary connection is established from one point via one or more segments.

Synchronous Data Link Control (SDLC): A discipline conforming to subsets of the Advanced Data Communications Control Procedures (ADCCP) of the American National Standards Institute (ANSI) and High-level Data Link Control (HDLC) of the International Organization for Standardization, for managing synchronous, code-transparent, serial-by-bit information transfer over a link connection. Transmission exchanges may be duplex, or half-duplex over switched or nonswitched links. The configuration of the link connection may be point-to-point, multipoint, or loop.

Synchronous Transmission: The transmission of data which involves sending a group of characters in a packet. This is a common method of transmission between computers on a network or between modems. One or more synchronous characters are transmitted to confirm clocking before each packet of data is transmitted. Compare to Asynchronous Transmission.

Systems Network Architecture (SNA): The description of the logical structure, formats, protocols, and operational sequences for transmitting information units through, and controlling the configuration and operation of networks.

T

Tariff: The rate/availability schedule for telephone and ISDN services from a regulated service provider.

TCP/IP: A set of communication protocols that support peer-to-peer connectivity functions for both local and wide area networks.

T Carrier: The generic name for a digitally multiplexed carrier system. In the North American digital hierarchy, a T is used to designate a DS (digital signal) level hierarchy. Examples: T1 (DS1) is a 1.544 M bps 24-channel designation. In Europe, T1 is called E1. The T Carrier system was originally designed for transmitting digitized voice signals, but has since been adapted for digital data applications.

T1: A digital transmission link capable of 1.544M bps. T1 uses two pairs of normal UTP, and can handle 24 voice conversations, each digitized at 64 Kbps. T1 is a standard for digital transmission in the U.S., Canada, Japan and Hong Kong. T1 is the access method for high-speed services such as ATM, frame relay, and SMDS. See also T Carrier, T1 line and FT1.

T1 Channel Tests: A set of diagnostics that vary by carrier, used to verify a T1 channel operation. Can include Tone, Noise Level, Impulse Noise Level, Echo Cancelers, Gain, and Crosstalk testing.

T1 Framing: To digitize and encode analog voice signals requires 8000 samples per second (twice the highest voice frequency of 4000 Hz). Encoding in an 8-bit word provides the basic T1 block of 64 Kbps for voice transmission. This "Level 0 Signal, as its called, is represented by "DS-0", or Digital Signal at Level 0. 24 of these voice channels are combined into a serial bit stream (using TDM), on a frame-by-frame basis. A frame is a sample of all 24 channels; so adding in a framing bit gives a block of 193 bits (24x8+1=193). Frames are transmitted at 8000 per second (the required sample rate), creating a 1.544M (8000x193=1.544M) transmission rate.

T1 Line: A digital communications facility that functions as a 24-channel pathway for data or voice transmission. A T1 line is composed of two separate elements: the Access element and the Long Haul element.

T1 Mux: A device used to carry many sources of data on a T1 line. The T1 mux assigns each data source to distinct DS0 time slots within the T1 signal. Wide bandwidth signals take more than one time slot. Normal voice traffic or 56/64 Kbps data channels take one time slot. The T1 mux may use an internal or external T1 DSU; a "channel bank" device typically uses an external T1 CSU.

Transmission Control Protocol / Internet Program (TCP/IP): A multi-layer set of protocols developed by the US Department of Defense to link dissimilar computers across dissimilar and unreliable LANs.

Terminal: The screen and keyboard device used in a mainframe environment for interactive data entry. Terminals have no "box", which is to say they have no file storage or processing capabilities.

Terminal Adapter (TA): An ISDN DTE device for connecting a non-ISDN terminal device to the ISDN network. Similar to a protocol converter or an interface converter, a TA connects a non-ISDN device between the R and S interfaces. Typically a PC card.

Terminal Endpoint Identifier (TEI): Up to eight devices can be connected to one ISDN BRI line. The TEI defines for a given message which of the eight devices is communicating with the Central Office switch. In general, more than one of the eight may be communicating.

Tie line: A dedicated circuit linking two points without having to dial a phone number (i.e., the line may be accessed by lifting the telephone handset or by pushing a button).

Time-Division Multiplexing (TDM): Division of a transmission facility into two or more channels by allotting the common channel to several different information channels, one at a time.

Time Slot: One of 24 channels within a T1 line. Each channel has a 64 Kbps maximum bandwidth. "Time slot" implies the time division multiplexing organization of the T1 signal.

Toll Call: A call to a location outside of your local service area (i.e., a long distance call).

Tone dialing: One of two methods of dialing a telephone, usually associated with Touch-Tone® (push button) phones. Compare with pulse dialing.

Topology: Physical layout of network components (cables, stations, gateways, and hubs). Three basic interconnection topologies are star, ring, and bus networks.

Transmission Control Protocol (TCP): A communications protocol used in Internet and in any network that follows the US Department of Defense standards for internetwork protocol. TCP provides a reliable host-to-host protocol between hosts in packet-switched communications networks and in interconnected systems of such networks. It assumes that the Internet protocol is the underlying protocol.

Transport Layer: Layer 4 of the Open Systems Interconnection (OSI) model; provides reliable, end-to-end delivery of data, and detects transmission sequential errors.

Transport Protocol Data Unit (TPDU): A transport header, which is added to every message, contains destination and source addressing information that allows the end-to-end routing of messages in multi-layer NAC networks of high complexity. They are automatically added to messages as they enter the network and can be stripped off before being passed to the host or another device that does not support TPDU's.

Trunk: Transmission links that interconnect switching offices.

TSR (terminate and stay resident): A software program that remains active and in memory after its user interface is closed. Similar to a daemon in UNIX environments.

Tunneling: Encapsulation data in an IP packet for transport across the Internet.

Twisted pair wiring: A type of cabling with one or more pairs of insulated wires wrapped around each other. An inexpensive wiring method used for LAN and telephone applications, also called UTP wiring.

U

UART (Universal Asynchronous Receiver/Transmitter) (pronounced "you art"): A chip that transmits and receives data on the serial port. It converts bytes into serial bits for transmission, and vice versa, and generates and strips the start and stop bits appended to each character.

UNIX: An operating system developed by Bell Laboratories that features multiprogramming in a multi-user environment.

Unshielded Twisted Pair (UTP): Telephone-type wiring. Transmission media for 10Base-T.

User Datagram Protocol (UDP): A TCP/IP protocol describing how messages reach application programs within a destination computer. This protocol is usually bundled with IP-layer software. UDP is a transport layer, connectionless mode protocol, providing a (potentially unreliable, unsequenced, and/or duplicated) datagram mode of communication for delivery of packets to a remote or local user.

V

V.25bis: An ITU-T standard for synchronous communications between a mainframe or host and a modem using HDLC or other character-oriented protocol.

V.54: The ITU-T standard for local and remote loopback tests in modems, DCEs and DTEs. The four basic tests are:

- local digital loopback (tests DTE send and receive circuits),
- local analog loopback (tests local modem operation),
- remote analog loopback (tests comm link to the remote modem), and
- remote digital loopback (tests remote modem operation).

Virtual Circuit: A logical connection. Used in packet switching wherein a logical connection is established between two devices at the start of transmission. All information packets follow the same route and arrive in sequence (but do not necessarily carry a complete address).

W

Wide Area Network (WAN): 1. A network that provides communication services to a geographic area larger than that served by a local area network or a metropolitan area network, and that may use or provide public communication facilities. 2. A data communications network designed to serve an area of hundreds or thousands of miles; for example, public and private packet-switching networks, and national telephone networks. Contrast with local area network (LAN).

Wide Area Telecommunications Service (WATS): A low-cost toll service offered by most long distance and local phone companies. Incoming (800 call service, or IN-WATS) and outgoing WATS are subscribed to separately, but over the same line.

X

X.25: ITU-T's definition of a three-level packet-switching protocol to be used between packet-mode DTEs and network DCEs. X.25 corresponds with layer 3 of the 7-layer OSI model.

Y

Yellow Alarm: An error indication sent by the T1 device when it has not gotten a receive signal, or cannot synchronize on the receive signal received. Contrast "Red Alarm" and "Blue Alarm".

Z

Zero Byte Time Slot Interchange (ZBTSI): A method for allowing 64 Kbps unrestricted user data (allowing all 0s in the user data). An alternative to (but not as popular as) B8ZS.

Index

A

About the Internet	94
Accessories, ordering	94
Adding ProxyServer applications	42
Adding RAM, MTPSR3-200	14
Answer command	102
Assigning IP addresses	28
Asynchronous Communications Mode command	106
Asynchronous gateway	38
AT commands	
%B	107
%C	107
&&S	108
&B	105
&C	105
&D	105
&F	105
&G	105
&J	105
&K	105
&M	106
&Q	106
&S	106
&T	106
&V	106
&W	106
&Y	106
&Z=	106
+++AT<CR>	102
+ES=	108
-C	107
\G	106
\J	106
\K	107
\N	107
\Q	107
\V	107
\X	107
A	102
A/	102
AT	102
B	102
C	102
E	103
F	103
H	103
L	103
M	104
N	104
O	104
Q	104
S=	104
S?	104
V	104
X	104
Y	105
Z	105

AT&T's "call card" tones	102, 103
Attention code	102
Autorun	16
Auxiliary Relay Control command	105

B

Back panel connectors	9
BBS	93
Bell 212A mode	102
Blacklist	107
Break signal	107

C

Cabling diagrams	96
Cabling the MTPSR3-200	13
Carrier Control command	102
CD-ROM, software installation	16
Changing Internet parameters	39
Changing IP Parameters	28
Changing ProxyServer configuration, overview	26
Changing the configuration of a remote unit	80
Changing WAN Port Parameters	31
Client only WAN port	28
Client Setup	52
Configuring in Windows 95/98	53
Configuring in Windows NT	61
Installing TCP/IP (Win95/98)	60
Installing TCP/IP (WinNT)	67
Overview	52
Command port cable	96
Command port connector	9
Communication Standard command	102
Communications Mode command	106
Configuration, AT command	
selecting	106
storing	106
viewing	106
Configuration Port Setup	26
Configuration Utilities	26
Configuring	
the Modem-Sharing Software	70
Connectors	9
Contacting Tech Support via E-mail	91

D

Data Buffer Control command	106
Data buffering	106
Data Calling Tone command	107
Data Compression Control command	107
Data mode	104
DCD Control command	105
Default settings	105
Detect AT&T's "call card" tone	102
DHCP, enable in IP Setup	28

DHCP server, setup	41
Diagnostics, running	49, 50
Dial Command	102
Dial Stored Telephone Number Command	103
DNS, enable in IP Setup	29
Domain Name Server (DNS)	111
Download Firmware	26
DSR Control command	106
DTR Control command	105
Dynamic bandwidth allocation	32

E

Echo Command Mode Characters command	103
Echo Online Data Characters command	103
Electrical specifications	10
Enable Synchronous Buffered Mode command	108
Enabling remote servers	47
Enabling the DHCP server	41
Enabling the virtual server	44
ENTER key	102
Error Correction Mode Selection command	107
Escape sequence	102
Establishing IP addressing	28
Ethernet 10Base-2 connector	9
Ethernet 10Base-T connector	9
Ethernet LEDs	8

F

Fail LED	8
Fallback	104
Flow control	105, 106, 107
Front panel, LEDs	8
FTP, changing values	43

G

Guard tone	105
------------------	-----

H

H.324	108
Handshake	104
Hanging up	102, 103
Hook Control command	103

I

Inactivity Timer	107
Information Request Command	103
Installing SIMM	14
Installing TCP/IP (Win95/98)	60
Installing TCP/IP (WinNT)	67
Internet	94
Internet Protocol (IP) defined	111
InterNIC, calling	111
IP Setup	28
IP Wizard setup	19

L

LAN cables	96
LAN-based remote configuration	80
Limited Warranty	90

On-line Warranty Registration	90
Link Connectors	9
Links 1, 2, 3 (LEDs)	8
Load Factory Default Settings command	105
Local Flow Control Selection command	105, 107
Long Space Disconnect command	105

M

Mapping IP addresses and domain names	111
Message Printing Control	39
MLPPP	36, 39, 40
MNP 5 data compression	107
MNP error correction	107
Modem Port Flow Control command	106
Modem Reset command	105
Modulation Handshake command	104
Monitor Speaker Mode command	104
Monitor Speaker Volume command	103
MTPSR3-200	
Accessories, ordering	94
Adding RAM	14
Back panel connectors	9
Cabling	13
Changing the configuration, overview	26
Front panel LEDs	8
Loading ProxyServer software	16
Overview	6
Service, warranty, and tech support	90
Specifications	10
Unpacking	12
Multi-Tech BBS	93
Multi-Tech Installation CD	16
MultiLink PPP	20
Multiple workstations	32

O

On-hook/off-hook	103
On-line command mode	104
On-line Warranty Registration	90
Operating system requirements	10
Ordering accessories	94

P

Physical specifications	10
Point-to-Point Protocol (PPP)	39
Port type	38
Power connector	9
Power LED	8
PPP, WAN links	39
Primary Server	29
Protocol Result Code command	107
ProxyServer applications, configuration	42
ProxyServer management	85
ProxyServer program group	26
ProxyServer software	26
Adding ProxyServer applications	42
Changing Internet parameters	39
Changing IP parameters	28
Changing WAN port parameters	31
Enabling remote servers	47
Enabling the DHCP server	41

Enabling the virtual server	44
Proxy setup	27
Running diagnostics	49, 50
Running statistics	50
ProxyServer Telnet server menu	84

R

RAS Dial-Out Redirector	
Installing WINMCSI modem-sharing software	70
Overview	70
Running WINMCSI workstation software	76
RAS enable option	28
RASExpress	36
Read Register Value command	104
Recording ProxyServer Information	91
Regulatory information	99
Canadian limitations notice	101
EMC and safety directive compliance	101
FCC Part 15	99
FCC regulation for telephone line interconnection	100
Remote configuration	80
Remote configuration cable	96
Remote User Database	
Setting up	22
Using	86
Repeat last command	102
Requirements, operating system	10
Resetting the modem	105
Result Code Format command	104
Result Code Selection command	104
Result codes	107
Result Codes Enable/Disable command	104
Retrain	105
Return Online to Data Mode command	104
RFC 1700	42

S

S-registers	
reading	104
setting	104
Scripting	
Commands (by function)	97
Example script	98
Secondary Server	29
Select Stored Configuration command	106
Self-Test commands	106
Service	92
Set Break Control command	107
Set Register Value command	104
Sharing resources	33
SIMM, installation	14
Single streamed applications	32
Software	
Description	26
Loading	16
Speaker Codec Loopback command	108
Speaker, controlling	103, 104
Specifications, technical	10
Speed conversion (data buffer)	106
Static routes	29
Statistics, running	50
Store Current Configuration command	106

Store Telephone Number command	106
Storing	
telephone numbers	106
Synchronous buffered mode	108

T

TCP/IP	
Address Resolution Protocol	109
Common applications and utilities	110
Establish Internet addressing strategy	109
Internet Protocol (IP) defined	111
MAC addresses	109
Overview	109
Stack	16, 80
User Datagram Protocol (UDP)	109
Tech Support	91
Contacting Tech Support via E-mail	91
Recording ProxyServer Information	91
Telnet	
Client	84
Dial-out	85
Enabling remote servers	47
ProxyServer configuration	85
ProxyServer management	85
Remote User Database	86
Server Menu	84
Testing	106, 108
Testing DSP 56K Code version/Checksum Command	108
Testing External RAM Command	108
Testing DSP 56K Code Version/Checksum	108
TFTP	47

U

Uninstall Proxy Server Configuration	26
Unpacking the MTPSR3-200	12
User Datagram Protocol (UDP)	109

V

V.22 mode	102
V.22bis Guard Tone command	105
V.25	107
V.32 Auto Retrain command	105
V.42 error correction	107
V.42bis data compression	107
Video	108
View Current Configuration command	106
View Numbers in Blacklist command	107
Virtual server	44
Virtual server, setup	45

W

WAN cables	96
WAN Device Configuration	26
WAN Link(s) setup	20
WEB Browser Management	87
WEB server	47
WINMCSI modem-sharing software	70
WINMCSI workstation software	76

X

XON/XOFF Pass-Through command 107